# CA IdentityMinder™

## Konfigurationshandbuch

12.6.3

# CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden CA-Produkte:

- CA IdentityMinder
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting
- CA GovernanceMinder

# Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

# Inhalt


## Kapitel 1: Einführung in CA IdentityMinder-Umgebungen 13

Komponenten der CA IdentityMinder-Umgebung ..... 13
Mehrere CA IdentityMinder-Umgebungen ..... 15
CA IdentityMinder-Management-Konsole ..... 16
Zugreifen auf die CA IdentityMinder-Management-Konsole ..... 16
So wird eine CA IdentityMinder-Umgebung erstellt ..... 17

## Kapitel 2: Beispiel einer CA IdentityMinder-Umgebung 19

Übersicht des Beispiels einer CA IdentityMinder-Umgebung ..... 19
So wird das NeteAuto-Beispiel mit Organisations-Support konfiguriert ..... 20
- LDAP-Verzeichnisstruktur für NeteAuto ..... 20
- Relationale Datenbank für NeteAuto ..... 21
- Erforderliche Software für NeteAuto ..... 22
- Installationsdateien für die NeteAuto-Umgebung ..... 22
- Installieren Sie die NeteAuto-Umgebung ..... 23
- Konfigurieren Sie ein LDAP-Benutzerverzeichnis. ..... 23
- Konfigurieren einer relationalen Datenbank ..... 24
- Erstellen des CA IdentityMinder-Verzeichnisses ..... 25
- Erstellen der NeteAuto-CA IdentityMinder-Umgebung ..... 27

So wird das NeteAuto-Beispiel ohne Organisations-Support konfiguriert ..... 30
- Beschreibung der CA IdentityMinder-Beispielumgebung ..... 30
- Installationsdateien für die NeteAuto-Umgebung ..... 31
- So wird die NeteAuto-Umgebung installiert - Ohne Organisations-Support ..... 32
- Erforderliche Software ..... 33
- Konfigurieren einer relationalen Datenbank ..... 33
- Erstellen des CA IdentityMinder-Verzeichnisses ..... 34
- Erstellen der NeteAuto-CA IdentityMinder-Umgebung ..... 36

So wird die NeteAuto-CA IdentityMinder-Umgebung verwendet ..... 37
- Verwaltung der Self-Service-Aufgaben ..... 38
- Benutzerverwaltung ..... 41

So werden zusätzliche Funktionen konfiguriert ..... 46
Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen ..... 46

## Kapitel 3: Verwaltung des LDAP-Benutzerspeichers 47

CA IdentityMinder-Verzeichnisse ..... 47
So erstellen Sie ein CA IdentityMinder-Verzeichnis ..... 48

Verzeichnisstruktur ..... 48
Verzeichniskonfigurationsdatei ..... 50
So wählen Sie eine Verzeichnis-Konfigurations-Vorlage aus ..... 51
So wird ein Benutzerverzeichnis für CA IdentityMinder beschrieben ..... 53
    So wird die Verzeichniskonfigurationsdatei geändert ..... 53
Verbindung zum Benutzerverzeichnis ..... 54
    Provider-Element ..... 55
Verzeichnissuchparameter ..... 58
Beschreibungen der über Benutzer, Gruppe und Organisation verwalteten Objekte ..... 60
    Beschreibung von verwalteten Objekten ..... 60
    Attributbeschreibungen ..... 65
    Verwalten vertraulicher Attribute ..... 71
    CA Directory - Überlegungen ..... 77
    Microsoft Active Directory-Überlegungen ..... 78
    IBM-Verzeichnisserver-Überlegungen ..... 78
    Oracle Internet Directory-Überlegungen ..... 79
Bekannte Attribute für einen LDAP-Benutzerspeicher ..... 79
    Bekannte Attribute für Benutzer ..... 80
    Bekannte Attribute für Gruppen ..... 83
    Bekannte Attribute zur Organisation ..... 85
    Attribut %ADMIN_ROLE_CONSTRAINT% ..... 86
    Konfigurieren von bekannten Attributen ..... 86
Beschreiben der Benutzerverzeichnisstruktur ..... 87
    So beschreiben Sie eine hierarchische Verzeichnisstruktur ..... 87
    So beschreiben Sie eine flache Benutzerverzeichnisstruktur ..... 87
    So beschreiben Sie eine flache Verzeichnisstruktur ..... 87
    So beschreiben Sie ein Benutzerverzeichnis, das keine Organisationen unterstützt ..... 88
So konfigurieren Sie Gruppen ..... 88
    Konfigurieren von selbstabonnierenden Gruppen ..... 88
    Konfigurieren von dynamischen und verschachtelten Gruppen ..... 89
    Hinzufügen von Unterstützung für Gruppen als Gruppenadministrator ..... 91
Validierungsregeln ..... 91
Zusätzliche Eigenschaften des CA IdentityMinder-Verzeichnisses ..... 92
    Konfigurieren der Sortierreihenfolge ..... 92
    Suchen über mehrere Objektklassen ..... 93
    Angeben der Wartezeit für Replikationen ..... 94
    Angeben von LDAP-Verbindungseinstellungen ..... 95
So verbessern Sie die Leistung von Verzeichnissuchen ..... 96
    So verbessern Sie die Leistung von großen Suchen ..... 97
    Konfigurieren von Paging-Unterstützung für Sun Java System Directory Server ..... 99
    Konfigurieren von Paging-Unterstützung für Active Directory ..... 100

## Kapitel 4: Verwaltung relationaler Datenbanken 103


CA IdentityMinder-Verzeichnisse ..... 103
Wichtige Hinweise für die Konfiguration von CA IdentityMinder für relationale Datenbanken ..... 105
Erstellen einer Oracle-Datenquelle für WebSphere ..... 106
So erstellen Sie ein CA IdentityMinder-Verzeichnis ..... 107
So erstellen Sie eine JDBC-Datenquelle ..... 107
- Erstellen einer JDBC-Datenquelle für JBoss-Anwendungsserver ..... 108
- Erstellen einer JDBC-Datenquelle für WebLogic ..... 111
- WebSphere-Datenquellen ..... 112

So erstellen Sie eine ODBC-Datenquelle für die Verwendung mit SiteMinder ..... 115
So beschreiben Sie eine Datenbank in einer Verzeichniskonfigurationsdatei ..... 115
- Ändern der Verzeichniskonfigurationsdatei ..... 117
- Beschreibung von verwalteten Objekten ..... 118
- So ändern Sie Attributbeschreibungen ..... 123

Verbindung zum Benutzerverzeichnis ..... 138
- Beschreibung einer Datenbankverbindung ..... 139
- SQL-Abfrageschemen ..... 142

Bekannte Attribute für eine relationale Datenbank ..... 144
- Bekannte Attribute für Benutzer ..... 145
- Bekannte Attribute für Gruppen ..... 147
- Attribut %Admin_Role_Constraint% ..... 148
- Konfigurieren von bekannten Attributen ..... 149

So konfigurieren Sie selbstabonnierende Gruppen ..... 149
Validierungsregeln ..... 151
Organisationsverwaltung ..... 151
- So richten Sie die Unterstützung von Organisationen ein ..... 151
- Konfigurieren der Unterstützung von Organisationen in der Datenbank ..... 152
- Spezifikation der Stammorganisation ..... 152
- Bekannte Attribute für Organisationen ..... 153
- So definieren Sie die Organisationshierarchie ..... 154

So verbessern Sie die Leistung von Verzeichnissuchen ..... 154
- So verbessern Sie die Leistung von großen Suchen ..... 155


## Kapitel 5: CA IdentityMinder-Verzeichnisse 157


Voraussetzungen zum Erstellen eines CA IdentityMinder-Verzeichnisses ..... 157
So erstellen Sie ein Verzeichnis ..... 158
Erstellen von Verzeichnissen mithilfe des Verzeichniskonfigurations-Assistenten ..... 158
- Starten des Verzeichniskonfigurations-Assistenten ..... 159
- Bildschirm "Select Directory Template" (Verzeichnisvorlage auswählen) ..... 161
- Fenster "Verbindungsdetails" ..... 161
- Konfigurieren des Fensters der verwalteten Objekte ..... 164

Bestätigungs-Fenster ... 171
Erstellen von Verzeichnissen mit einer XML-Konfigurationsdatei ... 172
Aktivieren von Bereitstellungsserver-Zugriff ... 174
Anzeigen von CA IdentityMinder-Verzeichnissen ... 177
CA IdentityMinder-Verzeichniseigenschaften ... 178
Fenster "CA IdentityMinder Directory Properties" (Verzeichniseigenschaften) ... 179
Anzeigen von verwalteten Objekteigenschaften und Attributen ... 181
Validation Rule Sets (Validierungsregelsätze) ... 185
Aktualisieren von Einstellungen für ein CA IdentityMinder-Verzeichnis ... 187
Exportieren von CA IdentityMinder-Verzeichnissen ... 187
Aktualisieren von CA IdentityMinder-Verzeichnissen ... 188
Löschen von CA IdentityMinder-Verzeichnissen ... 189

## Kapitel 6: CA IdentityMinder-Umgebungen 191

CA IdentityMinder-Umgebungen ... 191
Voraussetzungen für das Erstellen von CA IdentityMinder-Umgebungen ... 192
Erstellen einer CA IdentityMinder-Umgebung ... 193
Zugreifen auf eine CA IdentityMinder-Umgebung ... 198
Konfigurieren einer Umgebung für die Bereitstellung ... 199
Konfigurieren des Inbound Administrators (Administrator für Eingehendes) ... 199
Herstellen einer Verbindung zwischen der Umgebung und dem Bereitstellungsserver ... 201
Konfigurieren der Synchronisierung im Bereitstellungsmanager ... 201
Importieren von benutzerdefinierten Bereitstellungsrollen ... 203
Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen" ... 203
So können Sie Connectors mithilfe von Connector Xpress erstellen und bereitstellen ... 204
Verwalten von Umgebungen ... 212
Ändern von CA IdentityMinder-Umgebungseigenschaften ... 212
Umgebungseinstellungen ... 216
Exportieren einer CA IdentityMinder-Umgebung ... 217
Importieren einer CA IdentityMinder-Umgebung ... 217
Neustarten einer CA IdentityMinder-Umgebung ... 218
Löschen einer CA IdentityMinder-Umgebung ... 219
Verwalten von Konfigurationen ... 220
Einrichten von Config Xpress ... 221
Laden einer Umgebung in Config Xpress ... 222
Verschieben von Komponenten aus einer Umgebung in eine andere ... 224
Veröffentlichen von PDF-Berichten ... 225
Anzeigen der XML-Konfiguration ... 226
Optimieren der Auswertung von Richtlinienregeln ... 227
Role and Task Settings (Rollen- und Aufgabeneinstellungen) ... 228
Exportieren von Rollen- und Aufgabeneinstellungen ... 228

Importieren von Rollen- und Aufgabeneinstellungen ... 229
Erstellen von Rollen und Aufgaben für dynamische Endpunkte ... 230
Ändern des Systemmanager-Kontos ... 230
Aufrufen des Status einer CA IdentityMinder-Umgebung ... 232
Fehlerbehebung in CA IdentityMinder-Umgebungen ... 233

## Kapitel 7: Erweiterte Einstellungen 235

Überprüfung ... 235
Business Logic Task-Handler ... 236
Automatisches Löschen von Kennwortfeldern beim Zurücksetzen des Benutzerkennworts ... 237
Ereignisliste ... 237
E-Mail-Benachrichtigungen ... 238
Ereignis-Listener ... 238
Identitätsrichtlinien ... 239
Logical-Attribute-Handler ... 239
Sonstiges ... 240
Benachrichtigungsregeln ... 241
Organisationsauswahl ... 241
Bereitstellung ... 242
Bereitstellungsverzeichnis ... 243
Ermöglichen der Erstellung von Sitzungspools ... 243
Ermöglichen der Kennwortsynchronisierung ... 244
Zuordnungen von Attributen ... 244
Eingehende Zuordnungen ... 244
Ausgehende Zuordnungen ... 245
Benutzerkonsole ... 245
Webservices ... 247
Workflow Properties (Workflow-Eigenschaften) ... 248
Work Item Delegation (Arbeitselement delegieren) ... 248
Workflow Participant Resolvers (Workflow-Teilnehmer-Resolver) ... 249
Importieren/Exportieren von benutzerdefinierten Einstellungen ... 249
Fehler wegen unzureichendem Speicher in Java Virtual Machine ... 250

## Kapitel 8: Überprüfung 251

So konfigurieren und generieren Sie Audit-Datenberichte ... 251
Überprüfen der Voraussetzungen ... 254
Ändern der Auditeinstellungsdatei ... 254
Aktivieren der Überwachung für eine Aufgabe ... 259
Bericht anfordern ... 260
Anzeigen des Berichts ... 263
Bereinigen der Audit-Datenbank ... 264

## Kapitel 9: Produktionsumgebungen 265

So migrieren Sie Admin-Rollen und Aufgabendefinitionen ... 265
So exportieren Sie Admin-Rollen und Aufgabendefinitionen ... 266
So importieren Sie Admin-Rollen und Aufgabendefinitionen ... 266
So prüfen Sie den Rollen- und Aufgabenimport ... 267
So migrieren Sie CA IdentityMinder-Designs ... 267
Aktualisieren von CA IdentityMinder in einer Produktionsumgebung ... 268
So migrieren Sie eine CA IdentityMinder-Umgebung ... 268
So exportieren Sie eine CA IdentityMinder-Umgebung ... 269
So importieren Sie eine CA IdentityMinder-Umgebung ... 270
So prüfen Sie die Migration einer CA IdentityMinder-Umgebung ... 270
Migrieren der Datei "iam_im.ear" für JBoss ... 270
Migrieren der Datei "iam_im.ear" für WebLogic ... 271
Migrieren der Datei "iam_im.ear" für WebSphere ... 272
Migrieren von Workflow-Prozessdefinitionen ... 274
Exportieren von Prozessdefinitionen ... 274
Importieren von Prozessdefinitionen ... 275

## Kapitel 10: CA IdentityMinder-Protokolle 277

So verfolgen Sie Probleme in CA IdentityMinder ... 277
So verfolgen Sie Komponenten und Datenfelder ... 279

## Kapitel 11: CA IdentityMinder-Schutz 283

Sicherheit an der Benutzerkonsole ... 283
Sicherheit an der Management-Konsole ... 284
Hinzufügen zusätzlicher Administratoren zur Management-Konsole ... 285
Deaktivieren der systemeigenen Sicherheit für die Management-Konsole ... 286
Schützen der Management-Konsole mit SiteMinder ... 286
Schützen einer vorhandenen Umgebung nach einem Upgrade ... 288
Schutz vor CSRF-Angriffen ... 289

## Kapitel 12: Integration von CA SiteMinder 291

SiteMinder und CA IdentityMinder ... 292
So schützen Sie Ressourcen ... 293
Übersicht über die Integration von SiteMinder und CA IdentityMinder ... 294
Konfigurieren des SiteMinder-Richtlinienspeichers für CA IdentityMinder ... 299
Konfigurieren einer relationalen Datenbank ... 300
Konfigurieren von Sun Java Systems Directory Server oder IBM Directory Server ... 300
Konfigurieren von Microsoft Active Directory ... 301

Konfigurieren von Microsoft ADAM ... 302
Konfigurieren von CA Directory Server ... 302
Konfigurieren von Novell eDirectory Server ... 304
Konfigurieren von Oracle Internet Directory (OID) ... 305
Prüfen des Richtlinienspeichers ... 305
Importieren des CA IdentityMinder-Schemas in den Richtlinienspeicher ... 306
Erstellen eines SiteMinder 4.X-Agentenobjekts ... 306
Exportieren der CA IdentityMinder-Verzeichnisse und Umgebungen ... 308
Löschen aller Verzeichnis- und Umgebungsdefinitionen ... 309
Aktivieren des SiteMinder-Richtlinienserver-Ressourcenadapters ... 310
Deaktivieren des systemeigenen CA IdentityMinder-Framework-Authentifizierungsfilter ... 311
Neustarten des Anwendungsservers ... 312
Konfigurieren einer Datenquelle für SiteMinder ... 312
Importieren der Verzeichnisdefinitionen ... 313
Aktualisieren und Importieren von Umgebungsdefinitionen ... 314
Installieren des Web-Proxyserver-Plug-ins ... 314
Installieren des Proxy-Plug-ins auf WebSphere ... 315
Installieren Sie das Proxy-Plug-in für JBoss. ... 323
Installieren des Proxy-Plug-ins auf WebLogic ... 327
Ordnen Sie den SiteMinder-Agenten einer CA IdentityMinder-Domäne zu ... 335
Konfigurieren des SiteMinder-Parameters "LogOffUrl" ... 336
Fehlerbehebung ... 336
Fehlende Windows-DLL ... 337
Falscher SiteMinder-Richtlinienserver-Speicherort ... 337
Falscher Admin-Name ... 338
Falscher geheimer Admin-Schlüssel ... 339
Falscher Agentenname ... 340
Falscher geheimer Agentenschlüssel ... 341
Kein Benutzerkontext in CA IdentityMinder ... 342
Fehler beim Laden der Umgebungen ... 344
CA IdentityMinder-Verzeichnis oder -Umgebung kann nicht erstellt werden ... 345
Benutzer kann sich nicht anmelden ... 346
So konfigurieren Sie CA IdentityMinder-Agent-Einstellungen ... 346
Konfigurieren der SiteMinder-Hochverfügbarkeit ... 347
Ändern der Richtlinienserver-Verbindungseinstellungen ... 348
Hinzufügen von mehreren Richtlinienservern ... 349
Auswählen von Lastenausgleich oder Failover ... 349
Entfernen von SiteMinder aus einer vorhandenen CA IdentityMinder-Bereitstellung ... 350
SiteMinder-Vorgänge ... 350
Erfassen von Benutzeranmeldeinformationen mithilfe eines benutzerdefinierten Authentifizierungsschemas ... 351
Importieren von Datendefinitionen in den Richtlinienspeicher ... 352

Planen von Zugriffsrollen ....353
Konfigurieren des LogOff-URI ....368
Aliasnamen in SiteMinder-Bereichen....370
Ändern eines SiteMinder-Kennworts oder gemeinsamen geheimen Schlüssels....371
Konfigurieren einer CA IdentityMinder-Umgebung zur Verwendung von unterschiedlichen Verzeichnissen für Authentifizierung und Autorisierung....373
So verbessern Sie die Leistung von LDAP-Verzeichnisvorgängen ....375

## Anhang A: FIPS 140-2-Kompatibilität 377

<FIPS> Übersicht ....377
Kommunikation....378
Installation....378
Herstellen einer Verbindung mit SiteMinder ....379
Schlüsseldatei-Speicherung....379
Das Kennwort-Tool....380
FIPS-Modus-Erkennung....382
Verschlüsselte Textformate ....383
Verschlüsselte Informationen ....383
FIPS-Modus-Protokollierung ....383

## Anhang B: Ersetzen von CA IdentityMinder Zertifikate durch SHA-2-signierte SSL-Zertifikate 385

Nützliche Befehle ....388

# Kapitel 1: Einführung in CA IdentityMinder-Umgebungen

Dieses Kapitel enthält folgende Themen:

Komponenten der CA IdentityMinder-Umgebung (siehe Seite 13)
Mehrere CA IdentityMinder-Umgebungen (siehe Seite 15)
CA IdentityMinder-Management-Konsole (siehe Seite 16)
Zugreifen auf die CA IdentityMinder-Management-Konsole (siehe Seite 16)
So wird eine CA IdentityMinder-Umgebung erstellt (siehe Seite 17)

## Komponenten der CA IdentityMinder-Umgebung

Eine CA IdentityMinder-*Umgebung* stellt die Ansicht eines Verwaltungs-Namespace dar, mit dem CA IdentityMinder-Administratoren Objekte wie Benutzer, Gruppen, oder Organisationen verwalten können. Diesen Objekten wird ein Satz zugehöriger Rollen und Aufgaben zugeordnet. Die CA IdentityMinder-Umgebung steuert die Verwaltung und die grafische Darstellung eines Verzeichnisses.

Ein einzelner Benutzerspeicher kann mehrere CA IdentityMinder-Umgebungen (siehe Seite 15) verknüpfen, um unterschiedliche Ansichten des Verzeichnisses zu definieren. Allerdings ist eine CA IdentityMinder-Umgebung nur mit einem Benutzerspeicher verknüpft.

CA IdentityMinder-Umgebungen enthalten folgende Elemente:

**Verzeichnis**

Beschreibt einen Benutzerspeicher für CA IdentityMinder. Ein Verzeichnis-Element umfasst Folgendes:

- Ein Zeiger zu einem Benutzerspeicher, in dem verwaltete Objekte wie Benutzer, Gruppen und Organisationen gespeichert werden.
- Metadaten, die beschreiben, wie verwaltete Objekte im Verzeichnis gespeichert werden, und deren Darstellung in CA IdentityMinder.

**Provisioning-Verzeichnis (optional)**

Speichert Daten, die für den Provisioning-Server relevant sind, um zusätzliche Konten in verwalteten Endpunkten zu verwalten. Es kann nur ein Provisioning-Verzeichnis mit einer Umgebung verknüpft werden.

**Hinweis:** Weitere Informationen zum Provisioning-Server oder zum Provisioning-Verzeichnis können Sie dem *Installationshandbuch* entnehmen.

**Benutzerkonsole**

Ermöglicht CA IdentityMinder-Administratoren, Aufgaben in einer CA IdentityMinder-Umgebung auszuführen.

**Aufgaben- und Rollendefinitionen**

Bestimmen Sie Benutzerberechtigungen in CA IdentityMinder und anderen Anwendungen. Die Aufgaben- und Rollendefinitionen sind anfänglich in der CA IdentityMinder-Umgebung verfügbar, wo sie Benutzern zugewiesen werden können.

Sie können die Standardrollen und -aufgaben mithilfe der Benutzerkonsole anpassen.

**Self-Service**

Damit können Benutzer ihre eigenen Konten zum Zugriff auf Ressourcen, wie etwa eine Kundenwebseite, erstellen und verwalten. Mit dem Self-Service können Benutzer außerdem ein temporäres Kennwort für den Fall anfordern, dass das aktuelle Kennwort vergessen wurde.

**Workflow-Definitionen**

CA IdentityMinder schließt Standard-Workflow-Definitionen ein, die die Genehmigung und Benachrichtigung für Benutzerverwaltungsaufgaben, wie etwa Erstellen von Benutzerprofilen oder Zuweisen von Benutzern zu Rollen oder Gruppen, automatisieren. Sie können die Standard-Workflow-Vorgänge in CA IdentityMinder ändern, um sämtliche Unternehmensanforderungen zu unterstützen.

**Designs**

Bestimmen Sie die Anzeige der CA IdentityMinder-Benutzeroberfläche.

**Benutzerdefinierte Funktionen**

Sie können CA IdentityMinder ändern, um Ihre Geschäftsanforderungen mithilfe des CA IdentityMinder-APIs anzupassen. Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

Jede CA IdentityMinder-Umgebung macht es erforderlich, dass ein oder mehrere Systemmanager die initialen Rollen und Aufgaben mithilfe der Benutzerkonsole spezifisch anpassen. Sobald ein Systemmanager die initialen Rollen und Aufgaben erstellt, kann der Manager den Benutzern in dieser Umgebung Administratorrechte gewähren. Die Benutzer werden zu Administratoren, welche die Benutzer, Gruppen oder Organisationen verwalten. Weitere Informationen finden Sie im *Administrationshandbuch*.

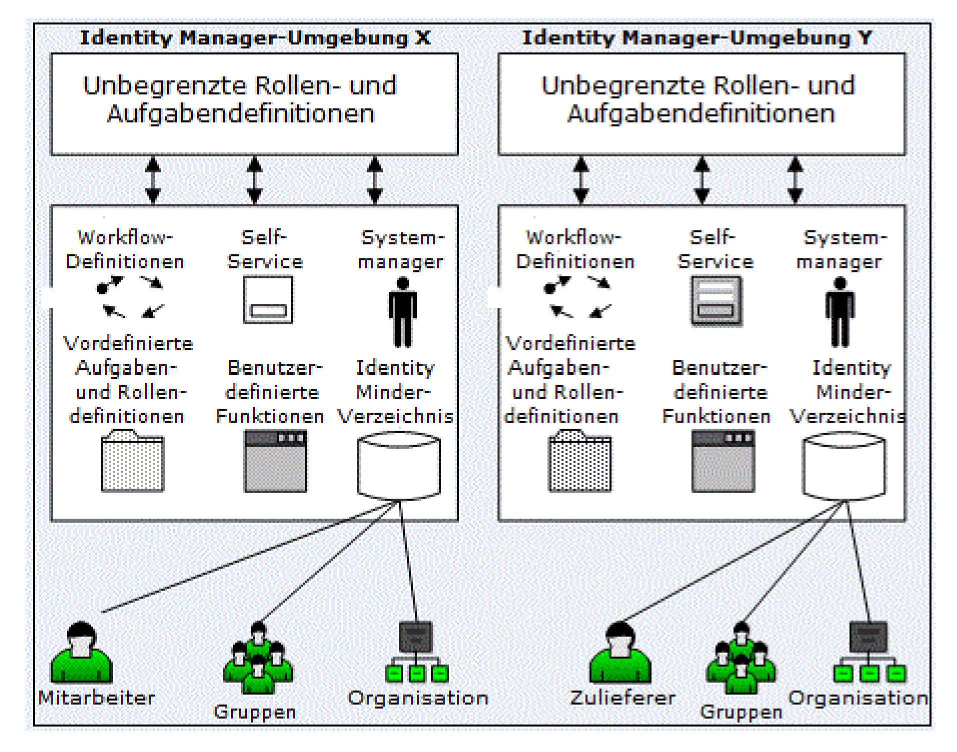
# Mehrere CA IdentityMinder-Umgebungen

Erstellen Sie mehrere CA IdentityMinder-Umgebungen, wenn Sie Folgendes möchten:

Verwalten zusätzlicher Benutzerspeicher - Sie können Benutzer in unterschiedlichen Typen von Benutzerspeichern verwalten. Beispiel: Ihr Unternehmen speichert all seine Benutzerprofile in einem Sun-Java-System-LDAP-Verzeichnis. Sie gehen ein Joint Venture mit einem Partner ein, der eine Oracle-Datenbank verwendet, um Benutzerinformationen zu speichern. Sie möchten jeweils eine andere CA IdentityMinder-Umgebung für jedes Set von Benutzern einsetzen.

- Verwalten Sie Objekte mit unterschiedlichen LDAP-Objektklassen. Ziehen Sie dabei in Betracht, dass CA IdentityMinder ein LDAP-Verzeichnis verwaltet. Innerhalb des gleichen Verzeichnisses können Sie Objekte des gleichen Typs mit verschiedenen Objektklassen und -attributen verwalten. Beispiel: Die folgende Abbildung zeigt ein Verzeichnis, das zwei Typen von Benutzern enthält:
  - Mitarbeiter, die eine Mitarbeiter-ID-Nummer haben.
  - Zulieferer, die mit einer Zuliefererzahl identifiziert werden.

*Equation 1: Das Diagramm zeigt ein Beispiel für zwei Identity Manager-Umgebungen mit Verzeichnissen, die Mitarbeiter und Zulieferer enthalten.*



# CA IdentityMinder-Management-Konsole

Als CA IdentityMinder-Systemadministrator umfassen Ihre Zuständigkeiten Folgendes:

- Erstellen eines CA IdentityMinder-Verzeichnisses
- Konfigurieren eines Provisioning-Verzeichnisses
- Konfigurieren einer CA IdentityMinder-Umgebung
- Zuweisen eines Systemmanagers
- Aktivieren benutzerdefinierter Funktionen für die Anfangsverwendung

Um eine CA IdentityMinder-Umgebung zu konfigurieren, verwenden Sie die Management-Konsole, eine webbasierte Anwendung.

Die Management-Konsole wird in die folgenden beiden Abschnitte unterteilt:

- Verzeichnisse - Verwenden Sie diesen Abschnitt, um CA IdentityMinder-Verzeichnisse und Provisioning-Verzeichnisse zu erstellen und zu verwalten, die die Benutzerspeicher für CA IdentityMinder erläutern.
- Umgebungen - Verwenden Sie diesen Abschnitt, um CA IdentityMinder-Umgebungen zu erstellen und zu verwalten, die die Verwaltungs- und Grafikpräsentationen eines Verzeichnisses steuern.

# Zugreifen auf die CA IdentityMinder-Management-Konsole

Um auf die Management-Konsole zuzugreifen, geben Sie die folgende URL in einen Browser ein:

http://*hostname:port*/iam/immanage

**Hostname**

Definiert den vollständig qualifizierten Domänennamen oder die IP-Adresse des Servers, auf dem CA IdentityMinder installiert ist.

**Hinweis**: Wenn Sie auf die Management-Konsole mithilfe von Internet Explorer 7 zugreifen und der Hostname eine IPv6-Adresse enthält, wird eine falsche Anzeige der Management-Konsole erwartet. Um dieses Problem zu vermeiden, verwenden Sie den vollständig qualifizierten Hostnamen oder eine IPv4-Adresse.

**port**

Definiert den Anwendungsserver-Port.

**Hinweis**: Wenn Sie einen Web-Agenten verwenden, um eine erweiterte Authentifizierung für CA IdentityMinder bereitzustellen, müssen Sie die Port-Nummer nicht angeben.

**Hinweis**: Aktivieren Sie JavaScript in dem Browser, den Sie verwenden, um auf die Management-Konsole zuzugreifen.

Beispiel-Pfade zur Management-Konsole:

- Für Geologic Weblogs:

  http://myserver.mycompany.org:7001/iam/immanage

- Für JBoss:

  http://myserver.mycompany.org:8080/iam/immanage

- Für WebSphere:

  http://myserver.mycompany.org:9080/iam/immanage

## So wird eine CA IdentityMinder-Umgebung erstellt

Um eine CA IdentityMinder-Umgebung zu erstellen, führen Sie die folgenden Schritte in der Management-Konsole aus:

1. Verwenden Sie den Assistenten für Verzeichniskonfiguration, (siehe Seite 158) um ein CA IdentityMinder-Verzeichnis zu erstellen.
2. Wenn Ihre Umgebung Bereitstellung einschließt, verwenden Sie den Assistenten für Verzeichniskonfiguration erneut, um ein Provisioning-Verzeichnis (siehe Seite 174) zu erstellen.
3. Erstellen Sie eine CA IdentityMinder-Umgebung.
4. Greifen Sie auf die Umgebung (siehe Seite 198) zu, um zu überprüfen, dass diese ausgeführt wird.

# Kapitel 2: Beispiel einer CA IdentityMinder-Umgebung

Dieses Kapitel enthält folgende Themen:

Übersicht des Beispiels einer CA IdentityMinder-Umgebung (siehe Seite 19)
So wird das NeteAuto-Beispiel mit Organisations-Support konfiguriert (siehe Seite 20)
So wird das NeteAuto-Beispiel ohne Organisations-Support konfiguriert (siehe Seite 30)
So wird die NeteAuto-CA IdentityMinder-Umgebung verwendet (siehe Seite 37)
So werden zusätzliche Funktionen konfiguriert (siehe Seite 46)
Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen (siehe Seite 46)

## Übersicht des Beispiels einer CA IdentityMinder-Umgebung

CA IdentityMinder umfasst eine Beispielumgebung, die Sie verwenden können, um CA IdentityMinder kennenzulernen und zu testen.

Als Beispielumgebung dient die Autohandelsgesellschaft namens NeteAuto. NeteAuto-Administratoren verwenden CA IdentityMinder, um Mitarbeiter, Zulieferer und regionale Verkaufsvertretungen zu verwalten.

Im Folgenden sind Benutzerspeicher-Konfigurationen zur Verwendung von NeteAuto-Beispielumgebungen aufgelistet:

- LDAP-Benutzerspeicher, die Organisationen unterstützen
- LDAP-Benutzerspeicher, die keine Organisationen unterstützen.
- Benutzerspeicher der relationalen Datenbanken, die Organisationen unterstützen
- Benutzerspeicher der relationalen Datenbanken, die keine Organisationen unterstützen.

**Hinweis**: Provisioning-Funktionen sind nicht verfügbar, da diese Umgebung kein Provisioning-Verzeichnis besitzt.

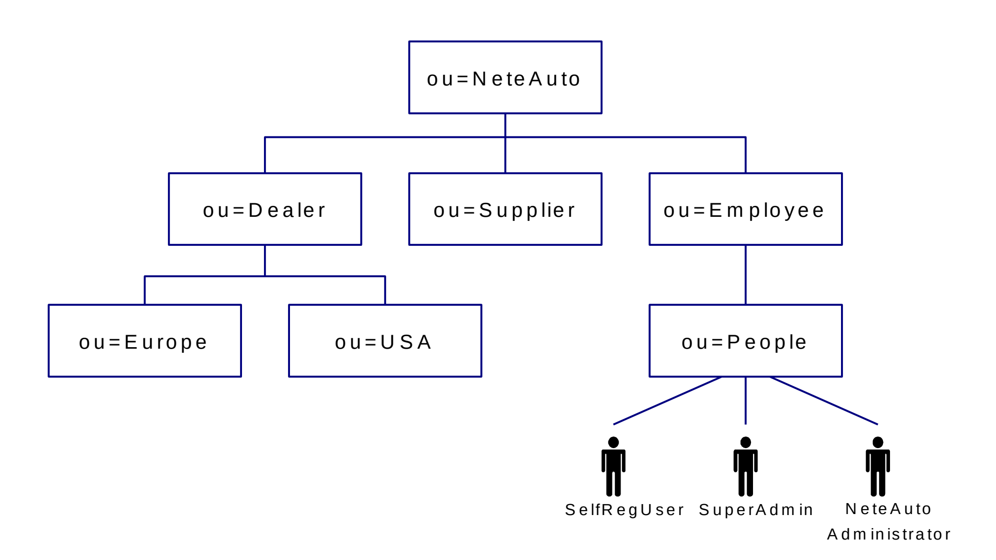
# So wird das NeteAuto-Beispiel mit Organisations-Support konfiguriert

Das Konfigurieren des NeteAuto-Beispiels mit Organisations-Support beinhaltet die folgenden Schritte:

- Installieren der erforderlichen Software
- Installieren der CA IdentityMinder-Beispielumgebung
- Konfigurieren eines LDAP-Benutzerverzeichnisses
- Konfigurieren einer relationalen Datenbank
- Erstellen des CA IdentityMinder-Verzeichnisses
- Erstellen der NeteAuto-CA IdentityMinder-Umgebung

## LDAP-Verzeichnisstruktur für NeteAuto

Die folgende Abbildung beschreibt das NeteAuto-Beispiel für LDAP-Verzeichnisse:




Die CA IdentityMinder-Beispielumgebung schließt die folgenden Benutzer ein:

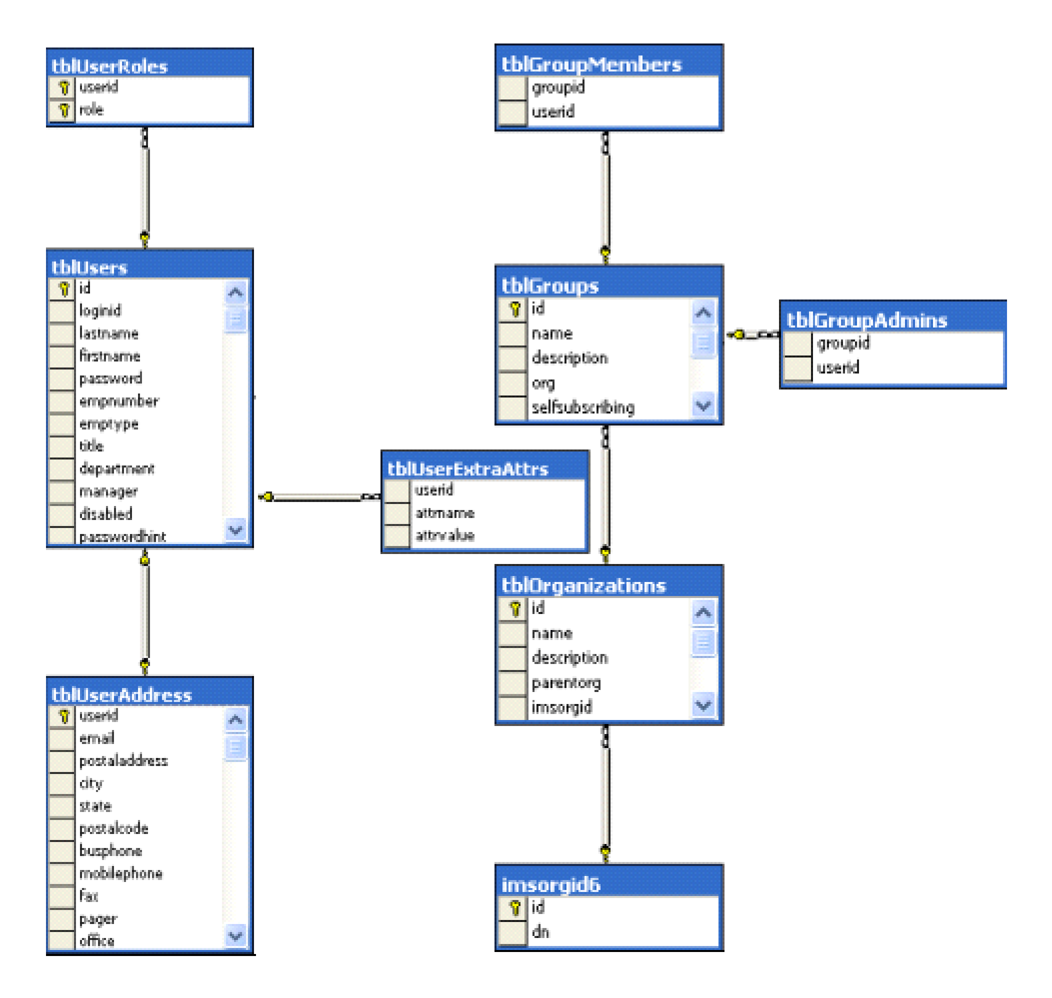
- Superadmin stellt das Administratorkonto mit der Systemmanager-Rolle für diese CA IdentityMinder-Umgebung dar. Als Superadmin können Sie alle standardmäßigen Admin-Aufgaben ausführen.

  **Hinweis:** Informationen über eine Beschreibung der standardmäßigen Admin-Aufgaben können Sie dem *Administrationshandbuch* entnehmen.

- SelfRegUser stellt das Administratorkonto dar, das CA IdentityMinder verwendet, um die Selbstregistrierung für die CA IdentityMinder-Umgebung zu aktivieren.
- NeteAuto-Administrator besitzt keine Berechtigungen, wenn Sie die NeteAuto-Umgebung installieren. Allerdings können Sie den Gruppenmanager als eine Benutzerrolle zuweisen, wie unter Zuweisen der Gruppenmanager-Rolle beschrieben.

## Relationale Datenbank für NeteAuto

Die folgende Abbildung beschreibt die relationale Datenbank für das NeteAuto-Beispiel einschließlich einer Organisationstabelle:



## Erforderliche Software für NeteAuto

Für die NeteAuto-CA IdentityMinder-Umgebung gelten die folgenden Voraussetzungen:

- Installieren Sie CA IdentityMinder, wie im *Installationshandbuch* beschrieben. Stellen Sie sicher, dass Sie die CA IdentityMinder-Admin-Tools installieren.
- Sie müssen Zugriff auf den Verzeichnisserver eines Sun Java-Systems (Sun ONE oder iPlanet) oder auf eine Microsoft SQL Server-Datenbank haben.

## Installationsdateien für die NeteAuto-Umgebung

CA IdentityMinder enthält ein Set von Dateien, die Sie verwenden können, um eine CA IdentityMinder-Beispielumgebung einzurichten. Die CA IdentityMinder-Umgebung stellt die Ansicht eines Verwaltungs-Namespace dar, der es CA IdentityMinder-Administratoren ermöglicht, Objekte wie Benutzer, Gruppen oder Organisationen zu verwalten. Diese Objekte werden zusammen mit einem Set von verknüpften Rollen und Aufgaben verwaltet. Die CA IdentityMinder-Umgebung steuert die Verwaltungs- und Grafikpräsentation eines Verzeichnisses.

Die CA IdentityMinder-Beispielumgebung umfasst Folgendes:

- Beispielobjekte, wie Benutzer und Organisationen
- Rollen-, Aufgaben- und Bildschirmdefinitionen

  Aufgaben werden in der Benutzerkonsole angezeigt, wenn Sie auf eine Registerkarte klicken, wie etwa für Benutzer oder Gruppen. Basierend auf den zugewiesenen Rollen werden die verknüpften Aufgaben angezeigt, wenn sich der Benutzer anmeldet.

  **Hinweis**: Weitere Informationen zu Rollen und Aufgaben finden Sie im *Administrationshandbuch*.

- Ein Beispieldesign, das die Benutzerkonsole für NeteAuto-Benutzer individuell anpasst.
- Eine Verzeichniskonfigurationsdatei, die Sie verwenden, um ein CA IdentityMinder-Verzeichnis zu erstellen.

Die Dateien für das Erstellen der CA IdentityMinder-Beispielumgebung werden unter dem folgenden Speicherort installiert:

*admin_tools*\samples\NeteAuto

In diesem Pfad bezieht sich *admin_tools* auf die Administrations-Tools. Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

## Installieren Sie die NeteAuto-Umgebung.

Führen Sie den folgenden Prozess aus, um die NeteAuto-Umgebung zu installieren.

**Gehen Sie wie folgt vor:**

1. Vergewissern Sie sich, dass die erforderliche Software installiert ist (siehe Seite 22).
2. Konfigurieren Sie den Benutzerspeicher, und importieren Sie die Beispieldaten.
   - Für LDAP-Benutzer: Konfigurieren Sie ein LDAP-Benutzerverzeichnis (siehe Seite 23)
   - Für Benutzer von relationalen Datenbanken: Konfigurieren Sie eine relationale Datenbank.
3. Erstellen Sie das NeteAuto-CA IdentityMinder-Verzeichnis.
4. Erstellen Sie die NeteAuto-CA IdentityMinder-Umgebung.
5. Konfigurieren Sie das Erscheinungsbild der CA IdentityMinder-Benutzeroberfläche für NeteAuto-Benutzer (siehe Seite 39).

## Konfigurieren Sie ein LDAP-Benutzerverzeichnis.

Das LDAP-Verzeichnis ist in Abhängigkeit von Ihrer Installation verfügbar. Sie können mit dem folgenden Verfahren überprüfen, ob das Verzeichnis vorhanden ist, oder Sie können das Verzeichnis erstellen.

**Gehen Sie wie folgt vor:**

1. Erstellen Sie in der Verzeichnisserverkonsole eine Instanz von LDAP mit folgendem Stamm:

   ```
   dc=security,dc=com
   ```

   Notieren Sie die Port-Nummer für zukünftige Referenzzwecke.

2. Importieren Sie die NeteAuto.ldif-Datei in den Verzeichnisserver von samples\NeteAuto in den Administrations-Tools.

   Die Verwaltungstools werden in den folgenden Standardordnern installiert:

   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

**Hinweis:** Wenn Sie beim Import der LDIF-Datei oder beim Erstellen des CA IdentityMinder-Verzeichnisses Probleme feststellen, fügen Sie den folgenden Text am Anfang der LDIF-Datei hinzu:

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

Speichern Sie die Datei, und wiederholen Sie die Schritte 1 und 2.

## Konfigurieren einer relationalen Datenbank

Führen Sie den folgenden Vorgang aus, um eine relationale Datenbank zu konfigurieren.

**Gehen Sie wie folgt vor:**

1. Erstellen Sie eine Datenbankinstanz mit der Bezeichnung "NeteAuto".
2. Erstellen Sie einen Benutzer names "neteautoadmin" mit dem Kennwort "test". Gewähren Sie NeteAuto neteautoadmin-Rechte (wie etwa public- oder db_owner-Rechte), indem Sie die Eigenschaften des Benutzers bearbeiten.

   **Hinweis:** Um eine NeteAuto-Datenbank zu erstellen, muss die Neteautoadmin-Rolle mindestens minimale Berechtigungen (auswählen, einfügen, aktualisieren und löschen) für alle Tabellen besitzen, die über by.sql-Skript erstellt werden. Außerdem muss neteautoadmin in der Lage sein, gegebenenfalls alle gespeicherten Prozeduren auszuführen, die in diesen Skripten definiert sind.
3. Wenn Sie Benutzereigenschaften bearbeiten, machen Sie NeteAuto zur Standarddatenbank für neteautoadmin.

4. Führen Sie die folgenden Skripte in der aufgelisteten Reihenfolge aus:
   - *db_type*-rdbuserdirectory.sql - Konfiguriert die Tabellen für das NeteAuto-Beispiel und erstellt die Benutzereingaben.
   - ims_*db_type*_rdb.sql - Konfiguriert den -Support für Organisationen

     *db_type*

     Definiert Microsoft SQL oder Oracle je nach Typ der Datenbank, die Sie konfigurieren.

   Diese Skriptdateien befinden sich im Ordner *admin_tools*\samples\NeteAutoRDB\Organization. In diesem Beispiel bezieht sich *admin_tools* auf die Administrations-Tools, die in den folgenden Standardspeicherorten installiert sind:
   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
5. Definieren Sie eine JDBC-Datenquelle mit der Bezeichnung "neteautoDS", die auf die NeteAuto-Datenbank verweist.

   Der Verfahren zum Konfigurieren einer Datenquelle hängt vom Typ des Anwendungsservers ab, auf dem CA IdentityMinder installiert ist. Der Abschnitt "So wird eine JDBC-Datenquelle erstellt (siehe Seite 107)" umfasst anwendungsserverspezifische Anweisungen zum Erstellen einer JDBC-Datenquelle.

## Erstellen des CA IdentityMinder-Verzeichnisses

Führen Sie den folgenden Vorgang aus, um ein CA IdentityMinder-Verzeichnis zu erstellen.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   http://*im_server:port*/iam/immanage

   ***im_server***

   Definiert den voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist.

   ***port***

   Definiert die Portnummer des Anwendungsservers.
2. Klicken Sie auf "Directories" (Verzeichnisse).
3. Klicken Sie auf "Create from Wizard" (Über Assistenten erstellen), um den CA IdentityMinder-Verzeichnisassistenten zu starten.

4. Suchen Sie nach der entsprechenden .xml-Datei der Verzeichniskonfiguration, und klicken Sie auf "Weiter".

   Hinweis: Die Verzeichniskonfigurationsdatei befindet sich in den folgenden Ordnern:

   ■ Für Benutzerverzeichnisse des Sun-Java-System-Verzeichnisservers:

     *admin_tools*\samples\NeteAuto\Organization\directory.xml

   ■ Für relationale Datenbanken:

     *admin_tools*\samples\NeteAutoRDB\Organization*db_type* directory.xml

     *admin_tools*

       Definiert den Installationsspeicherort der Administrations-Tools.

       Die Verwaltungstools werden in den folgenden Standardordnern installiert:

       **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools

       **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

     *db_type*

       Gibt den Typ der Datenbank an, die Sie konfigurieren: Microsoft SQL oder Oracle.

   Statusinformationen werden auf dem Ausgabebildschirm der Verzeichniskonfiguration angezeigt.

5. Stellen Sie auf der zweiten Seite des Assistenten die folgenden Werte bereit:

   ■ Sun Java System-Verzeichnisserver

     **Name**

       NeteAuto Directory (NeteAuto-Verzeichnis)

     **Description (Beschreibung)**

       Sample NeteAuto directory (NeteAuto-Beispielverzeichnis)

     **Connection Object Name (Name des Verbindungsobjekts)**

       NeteAuto Users (NeteAuto-Benutzer)

     **Host**

       Bestimmt den Namen oder die IP-Adresse des Systems, auf dem der Benutzerspeicher installiert ist.

     **Port**

       Port-Nummer für den Benutzerspeicher

     **Suchstamm**

       dc=security, dc=com

**Benutzername**

Benutzername für ein Konto, das auf den Benutzerspeicher zugreifen kann.

**Kennwort und Kennwortbestätigung**

Kennwort für das Benutzerkonto

- Microsoft SQL Server und Oracle-Datenbanken

  **Name**

  NeteAutoRDB Directory

  **Beschreibung**

  Sample NeteAuto directory (NeteAuto-Beispielverzeichnis)

  **Connection Object Name (Name des Verbindungsobjekts)**

  NeteAutoRDB

  **JDBC Data Source (JDBC-Datenquelle)**

  neteautoDS

  **Benutzername**

  Neteautoadmin

  **Kennwort**

  Test

6. Klicken Sie auf "Weiter".
7. Klicken Sie auf "Fertigstellen", um den Assistenten zu beenden.

## Erstellen der NeteAuto-CA IdentityMinder-Umgebung

Führen Sie den folgenden Vorgang aus, um die NeteAuto-CA IdentityMinder-Umgebung zu erstellen.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".
2. Klicken Sie im CA IdentityMinder-Umgebungs-Fenster auf "Neu".

   Der CA IdentityMinder-Umgebungs-Assistent wird angezeigt.
3. Geben Sie auf der ersten Seite des Assistenten die folgenden Werte ein:

   **Umgebungs-Name**

   NeteAuto-Umgebung

   **Beschreibung**

   Beispiel-Umgebung

**Alias**

NeteAuto

Das Alias wird der URL hinzugefügt, um auf die CA IdentityMinder-Umgebung zugreifen zu können. Die URL zum Zugriff auf die Neteauto-Umgebung kann beispielsweise wie folgt lauten:

http://*server_name*/iam/im/neteauto

*server_name*

Definiert den vollständig qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist. Beispiel:

http://myserver.mycompany.org/iam/im/neteauto

**Hinweis:** Beim Alias muss die Groß-/Kleinschreibung beachtet werden.

Klicken Sie auf "Weiter".

4. Wählen Sie das CA IdentityMinder-Verzeichnis aus, das mit der Umgebung zu verknüpfen ist, die Sie erstellen:
   - Verwenden Sie für den Verzeichnisserver des Sun-Java-Systems das NeteAuto-Verzeichnis.
   - Verwenden Sie für Microsoft SQL Server oder die Oracle-Datenbank das NeteAutoRDB-Verzeichnis.

   Klicken Sie auf "Weiter".

5. Konfigurieren Sie den Support für öffentliche Aufgaben, wie die Selbstregistrierung und die Aufgaben im Fall von vergessenen Kennwörtern, wie folgt:
   a. Geben Sie folgenden Alias für öffentliche Aufgaben ein:

      Neteautopublic
   b. Geben Sie SelfRegUser als anonymes Benutzerkonto ein.
   c. Klicken Sie auf "Bestätigen", um die für den Benutzer eindeutige Kennung anzuzeigen.

   **Hinweis:** Benutzer müssen sich nicht anmelden, um öffentliche Aufgaben verwenden zu können.

6. Wählen Sie die Aufgaben und Rollen, die für die NeteAuto-Umgebung zu erstellen sind:
   a. Wählen Sie Import-Rollen aus der Datei.
   b. Navigieren Sie zu einem der folgenden Speicherorte:
      - Für einen Benutzerspeicher des Sun-Java-System-Verzeichnisservers:

        *admin_tools*\samples\NeteAuto\RoleDefinitions.xml

- Für einen Benutzerspeicher des Microsoft SQL Servers:

  *admin_tools*\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml

- Für einen Benutzerspeicher von Oracle:

  *admin_tools*\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

*admin_tools* bezieht sich auf die Administrations-Tools, die standardmäßig unter folgendem Speicherort installiert sind:

**Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools

**UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. Geben Sie einen Benutzer an, der als Systemmanager für diese Umgebung fungieren soll, und klicken Sie auf "Weiter":
   a. Geben Sie "SuperAdmin" im Systemmanager-Feld ein.
   b. Klicken Sie auf "Hinzufügen".

      CA IdentityMinder fügt die eindeutige Kennung des Superadmin-Benutzers zur Liste der Benutzer hinzu.
   c. Klicken Sie auf "Weiter".
8. Überprüfen Sie die Einstellungen für die Umgebung, und führen Sie die folgenden Aufgaben aus:
   - (Optional) Klicken Sie zum Ändern auf "Vorherige".
   - Klicken Sie auf "Fertigstellen", um die CA IdentityMinder-Umgebung mit den aktuellen Einstellungen zu erstellen.

     Der Ausgabebildschirm der Umgebungskonfiguration zeigt den Fortschritt der Umgebungserstellung an.
9. Klicken Sie auf "Fortfahren", um den CA IdentityMinder-Umgebungsassistenten zu verlassen.
10. Starten Sie die CA IdentityMinder-Umgebung.

Wenn Sie die NeteAuto-Umgebung erstellen, können Sie folgendes tun:

- Erstellen Sie ein Design für diese CA IdentityMinder-Umgebung (siehe Seite 39).
- Greifen Sie auf die Umgebung zu. (siehe Seite 37)

# So wird das NeteAuto-Beispiel ohne Organisations-Support konfiguriert

Das Konfigurieren des NeteAuto-Beispiels ohne Organisations-Support beinhaltet die folgenden Schritte:

- Installieren der erforderlichen Software (siehe Seite 22)
- Installieren der CA IdentityMinder-Beispielumgebung
- Konfigurieren der Datenbank
- Erstellen der JDBC-Datenquelle
- Erstellen des CA IdentityMinder-Verzeichnisses
- Erstellen der NeteAuto-CA IdentityMinder-Umgebung

## Beschreibung der CA IdentityMinder-Beispielumgebung

Für Microsoft SQL Server und Oracle-Datenbanken enthält CA IdentityMinder eine Version der NeteAuto-Umgebung, die keine Organisationen umfasst. Diese CA IdentityMinder-Umgebung schließt die folgenden drei Benutzer ein:

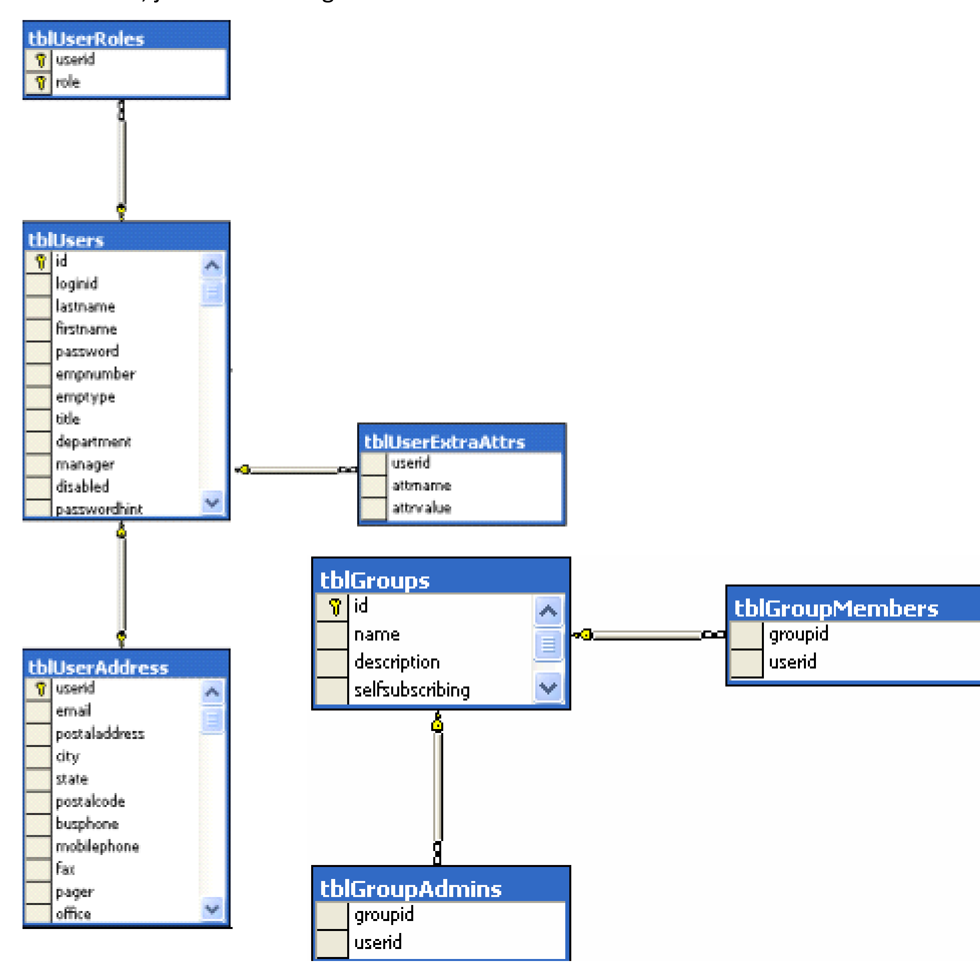
- Superadmin stellt das Administratorkonto mit der Systemmanager-Rolle für diese CA IdentityMinder-Umgebung dar. Als Superadmin können Sie alle standardmäßigen Admin-Aufgaben ausführen.

  **Hinweis:** Informationen über eine Beschreibung der standardmäßigen Admin-Aufgaben können Sie dem *Administrationshandbuch* entnehmen.

- SelfRegUser stellt das Administratorkonto dar, das CA IdentityMinder verwendet, um die Selbstregistrierung für die CA IdentityMinder-Umgebung zu aktivieren.
- NeteAuto-Administrator besitzt keine Berechtigungen, wenn Sie die NeteAuto-Umgebung installieren.

  Sie können jedoch dem NeteAuto-Administratorkonto die Gruppen-Manager-Rolle zuweisen.

Die folgende Abbildung beschreibt das NeteAuto-Beispiel für eine relationale Datenbank, jedoch ohne Organisationen:




## Installationsdateien für die NeteAuto-Umgebung

CA IdentityMinder enthält ein Set von Dateien, die Sie verwenden können, um eine CA IdentityMinder-Beispielumgebung einzurichten. Eine CA IdentityMinder-Umgebung stellt die Ansicht eines Verwaltungs-Namespace dar, der CA IdentityMinder-Administratoren zum Verwalten von Objekten befähigt. Diese Objekte wie Benutzer und Gruppen gehen mit einem Set von verknüpften Rollen und Aufgaben einher. Die CA IdentityMinder-Umgebung steuert die Verwaltungs- und Grafikpräsentation eines Benutzerspeichers.

Die CA IdentityMinder-Beispielumgebung umfasst Folgendes:

- Beispielbenutzer
- Rollen-, Aufgaben- und Bildschirmdefinitionen

  Aufgaben werden in der Benutzerkonsole angezeigt, wenn Sie auf eine Kategorie klicken, wie etwa für Benutzer oder Gruppen. Die Aufgaben, die angezeigt werden, basieren auf den Rollen, die dem Benutzer zugewiesen sind.

  **Hinweis**: Weitere Informationen zu Rollen und Aufgaben finden Sie im *Administrationshandbuch*.

- Ein Beispieldesign, das die Benutzerkonsole für NeteAuto-Benutzer individuell anpasst.
- Eine Verzeichniskonfigurationsdatei, die Sie verwenden, um ein CA IdentityMinder-Verzeichnis zu erstellen.

Die Dateien für das Erstellen der CA IdentityMinder-Beispielumgebung werden unter dem folgenden Speicherort installiert:

*admin_tools*\samples\NeteAutoRDB\NoOrganization

In diesem Pfad bezieht sich *admin_tools* auf die Administrations-Tools.

Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

## So wird die NeteAuto-Umgebung installiert - Ohne Organisations-Support

Führen Sie den folgenden Prozess aus, um die NeteAuto-Umgebung zu installieren.

**Gehen Sie wie folgt vor:**

1. Stellen Sie sicher, dass die erforderliche Software (siehe Seite 33) installiert ist.
2. Konfigurieren Sie die Datenbank (siehe Seite 24).
3. Erstellen Sie das CA IdentityMinder-Verzeichnis. (siehe Seite 34)
4. Erstellen Sie die NeteAuto-CA IdentityMinder-Umgebung (siehe Seite 36).
5. Konfigurieren Sie das Erscheinungsbild der CA IdentityMinder-Benutzeroberfläche für NeteAuto-Benutzer (siehe Seite 39).

## Erforderliche Software

Für die NeteAuto-CA IdentityMinder-Umgebung gelten die folgenden Voraussetzungen:

- Installieren Sie CA IdentityMinder, wie im *Installationshandbuch* beschrieben. Führen Sie eine Überprüfung durch, um die CA IdentityMinder-Admin-Tools zu installieren.
- Sie müssen Zugriff auf einen Microsoft SQL Server oder eine Oracle-Datenbank haben.

## Konfigurieren einer relationalen Datenbank

Führen Sie den folgenden Vorgang aus, um eine relationale Datenbank zu konfigurieren.

**Gehen Sie wie folgt vor:**

1. Erstellen Sie eine Datenbankinstanz mit der Bezeichnung "NeteAuto".
2. Erstellen Sie einen Benutzer names "neteautoadmin" mit dem Kennwort "test". Gewähren Sie NeteAuto neteautoadmin-Rechte (wie etwa public- oder db_owner-Rechte), indem Sie die Eigenschaften des Benutzers bearbeiten.

   **Hinweis:** Um eine NeteAuto-Datenbank zu erstellen, muss die Neteautoadmin-Rolle mindestens minimale Berechtigungen (auswählen, einfügen, aktualisieren und löschen) für alle Tabellen besitzen, die über by.sql-Skript erstellt werden. Außerdem muss neteautoadmin in der Lage sein, gegebenenfalls alle gespeicherten Prozeduren auszuführen, die in diesen Skripten definiert sind.
3. Wenn Sie Benutzereigenschaften bearbeiten, machen Sie NeteAuto zur Standarddatenbank für neteautoadmin.
4. Führen Sie die folgenden Skripte in der aufgelisteten Reihenfolge aus:
   - *db_type*-rdbuserdirectory.sql - Konfiguriert die Tabellen für das NeteAuto-Beispiel und erstellt die Benutzereingaben.
   - ims_*db_type*_rdb.sql - Konfiguriert den -Support für Organisationen

     *db_type*

       Definiert Microsoft SQL oder Oracle je nach Typ der Datenbank, die Sie konfigurieren.

   Diese Skriptdateien befinden sich im Ordner *admin_tools*\samples\NeteAutoRDB\Organization. In diesem Beispiel bezieht sich *admin_tools* auf die Administrations-Tools, die in den folgenden Standardspeicherorten installiert sind:

   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. Definieren Sie eine JDBC-Datenquelle mit der Bezeichnung "neteautoDS", die auf die NeteAuto-Datenbank verweist.

   Der Verfahren zum Konfigurieren einer Datenquelle hängt vom Typ des Anwendungsservers ab, auf dem CA IdentityMinder installiert ist. Der Abschnitt "So wird eine JDBC-Datenquelle erstellt (siehe Seite 107)" umfasst anwendungsserverspezifische Anweisungen zum Erstellen einer JDBC-Datenquelle.

## Erstellen des CA IdentityMinder-Verzeichnisses

Führen Sie das folgende Verfahren durch, um das CA IdentityMinder-Verzeichnis zu erstellen.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   http://*im_server*:*port*/iam/immanage

   *im_server*

   Definiert den voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist.

   *port*

   Definiert die Portnummer des Anwendungsservers.

2. Klicken Sie auf "Directories" (Verzeichnisse).

   Das Fenster der CA IdentityMinder-Verzeichnisse wird angezeigt.

3. Klicken Sie auf "Neu", um den CA IdentityMinder-Verzeichnisassistenten zu starten.

4. Suchen Sie nach einer der folgenden XML-Dateien der Verzeichniskonfiguration, und klicken Sie auf "Weiter":
   - Sun Java-Systeme:

     *admin_tools*\samples\NeteAuto\NoOrganization\directory.xml
   - SQL-Server-Datenbanken:

     *admin_tools*\samples\NeteAuto\NoOrganization\mssql-directory.xml
   - Oracle-Datenbanken:

     *admin_tools*\samples\NeteAuto\NoOrganization\oracle-directory.xml

   *admin_tools* bezieht sich auf die Administrations-Tools, die standardmäßig unter folgendem Speicherort installiert sind:
   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   Statusinformationen werden auf dem Ausgabebildschirm der Verzeichniskonfiguration angezeigt.
5. Stellen Sie auf der zweiten Seite des Assistenten die folgenden Werte bereit:

   **Name**

   NeteAutoRDB Directory

   **Beschreibung**

   NeteAuto-Beispielverzeichnis ohne Organisations-Support

   **Connection Object Name (Name des Verbindungsobjekts)**

   NeteAutoRDB

   **JDBC Data Source (JDBC-Datenquelle)**

   neteautoDS

   **Benutzername**

   neteautoadmin

   **Kennwort**

   test
6. Klicken Sie auf "Weiter".
7. Klicken Sie auf "Fertigstellen", um den Assistenten zu beenden.

## Erstellen der NeteAuto-CA IdentityMinder-Umgebung

Führen Sie den folgenden Vorgang aus, um die NeteAuto-CA IdentityMinder-Umgebung zu erstellen.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".
2. Klicken Sie im CA IdentityMinder-Umgebungs-Fenster auf "Neu".

   Der CA IdentityMinder-Umgebungs-Assistent wird geöffnet.

3. Geben Sie auf der ersten Seite des Assistenten die folgenden Werte ein:
   - Umgebungsname - NeteAuto-Umgebung
   - Beschreibung - NeteAuto stellt eine Beispielumgebung dar.
   - Alias - neteautoRDB

     Das Alias wird der URL hinzugefügt, um auf die CA IdentityMinder-Umgebung zugreifen zu können. Die URL zum Zugriff auf die Neteauto-Umgebung kann beispielsweise wie folgt lauten:

     `http://`*`domain`*`/iam/im/neteautoRDB`

     In diesem Pfad definiert die *Domäne* den vollständig qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist, wie im folgenden Beispiel verdeutlicht wird:

     `http://myserver.mycompany.org/iam/im/neteautoRDB`

     **Hinweis:** Beim Alias muss die Groß-/Kleinschreibung beachtet werden.

   Klicken Sie auf "Weiter".

4. Wählen Sie das CA IdentityMinder-Verzeichnis des NeteAutoRDB-Verzeichnisses aus, um es mit der Umgebung zu verknüpfen, die Sie erstellen. Klicken Sie anschließend auf "Weiter".
5. Konfigurieren Sie den Support für öffentliche Aufgaben, wie etwa die Selbstregistrierung und die Aufgaben im Fall von vergessenen Kennwörtern.

   **Hinweis:** Benutzer müssen sich nicht anmelden, um auf öffentliche Aufgaben zugreifen zu können.

   a. Geben Sie folgenden Alias für öffentliche Aufgaben ein:

      neteautoRDBpublic

   b. Geben Sie SelfRegUser als anonymes Benutzerkonto ein.

   c. Klicken Sie "Bestätigen", um die für Benutzer eindeutige Kennung anzuzeigen (2, in diesem Fall).

6. Wählen Sie die Aufgaben und Rollen, die für die NeteAuto-Umgebung zu erstellen sind:
   - Wählen Sie Import-Rollen aus der Datei.
   - Navigieren Sie zum folgenden Speicherort:

     *im_admin_tools_dir*\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

     In diesem Pfad definiert *im_admin_tools_dir* den installierten Speicherort der CA IdentityMinder-Admin-Tools.
7. Geben Sie einen Benutzer an, der als Systemmanager für diese Umgebung fungieren soll, und klicken Sie auf "Weiter":
   a. Geben Sie "SuperAdmin" im Systemmanager-Feld ein.
   b. Klicken Sie auf "Hinzufügen".
   c. Klicken Sie auf "Weiter".
8. Überprüfen Sie die Einstellungen für die Umgebung.
   - Klicken Sie zum Ändern auf "Vorherige".
   - Klicken Sie auf "Fertigstellen", um die CA IdentityMinder-Umgebung mit den aktuellen Einstellungen zu erstellen.

     Der Ausgabebildschirm der Umgebungskonfiguration zeigt den Fortschritt der Umgebungserstellung an.
9. Klicken Sie auf "Fertigstellen", um den CA IdentityMinder-Umgebungs-Assistenten zu verlassen.
10. Starten Sie die CA IdentityMinder-Umgebung.

Wenn Sie die NeteAuto-Umgebung erstellt haben, können Sie folgendes tun:

- Erstellen Sie ein Design für diese CA IdentityMinder-Umgebung, wie unter Setup des NeteAuto-Designs (siehe Seite 39) beschrieben.
- Greifen Sie auf die Umgebung wie unter "So wird die NeteAuto-CA IdentityMinder-Umgebung verwendet" beschrieben zu.

# So wird die NeteAuto-CA IdentityMinder-Umgebung verwendet

Sie können die NeteAuto-CA IdentityMinder-Umgebung verwenden, um Self-Service-Aufgaben und Benutzer zu verwalten.

## Verwaltung der Self-Service-Aufgaben

Die Self-Service-Aufgaben umfassen Folgendes:

- Registrieren als neuer Benutzer
- Anmelden als selbst registrierter Benutzer
- Verwenden der Funktion im Falle eines vergessenen Kennworts

### Als neuer Benutzer registrieren

Führen Sie den folgenden Vorgang aus, um sich als neuer Benutzer zu registrieren.

**Gehen Sie wie folgt vor:**

1. Geben Sie die folgende URL in einen Browser ein:

   `http://`*`hostname`*`/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   **Hostname**

   Definiert den vollständig qualifizierten Domänennamen des Systems, in dem CA IdentityMinder betrieben wird.

   **Hinweis:** Wurde die Konfiguration des NeteAuto-Design (siehe Seite 39) noch nicht durchgeführt, können Sie "imcss" aus der URL folgendermaßen weglassen:

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   Diese URL leitet Sie zur CA-Standardkonsole.

   Bei der Selbstregistrierung: Seite der Endbenutzer-Lizenzvereinbarung; CA IdentityMinder zeigt die CA-Website an.

   **Hinweis:** Sie können die standardmäßige Selbstregistrierungsaufgabe konfigurieren, um die benutzerdefinierte Endbenutzer-Lizenzvereinbarung anzuzeigen. Weitere Anweisungen finden Sie im *Administrationshandbuch*.

2. Klicken Sie auf "Akzeptieren", um fortzufahren.
3. Geben Sie auf der Registerkarte "Profil" die folgenden Details an:
   a. Geben Sie die Werte für die Mussfelder ein, welche mit einem Sternchen (*) versehen sind.
   b. Geben Sie Hinweise und Antworten für die Kennwortabfrage ein.

      Für den Fall eines vergessenen Kennworts stellt CA IdentityMinder einen Hinweis zum Kennwort bereit und fordert die Antwort an. Wenn die Antwort richtig ist, fordert CA IdentityMinder den Benutzer auf, ein neues Kennwort anzugeben und dieses zu bestätigen.
4. Lassen Sie die Registerkarte "Gruppen" unverändert.
5. Klicken Sie auf "Senden".

## Als selbst registrierter Benutzer anmelden

Führen Sie den folgenden Vorgang aus, um sich als ein selbst registrierter Benutzer anzumelden.

**Gehen Sie wie folgt vor:**

1. Geben Sie die folgende URL für die NeteAuto-CA IdentityMinder-Umgebung in einen Browser ein:

   `http://`*`hostname`*`/iam/im/neteauto/imcss/index.jsp`

   **Hostname**

   Definiert den vollständig qualifizierten Domänennamen des Systems, in dem CA IdentityMinder betrieben wird.

2. Melden Sie sich mit dem Benutzernamen und dem Kennwort an, die Sie bei der Registrierung angegeben haben.

## Richten Sie das NeteAuto-Design ein.

Um das NeteAuto-Design einzurichten, erstellen Sie eine SiteMinder-Antwort im SiteMinder-Richtlinienserver.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei einer der folgenden Schnittstellen als Administrator mit Domänenberechtigungen an:

   - Für CA SiteMinder Web Access Manager r12 oder höher melden Sie sich bei der Verwaltungsoberfläche an.
   - Für CA eTrust SiteMinder 6.0 SP5 melden Sie sich bei der Richtlinienserver-Benutzeroberfläche an.

   **Hinweis:** Weitere Informationen zur Verwendung dieser Schnittstellen finden Sie in der Dokumentation der SiteMinder-Version, die Sie verwenden.

2. Öffnen Sie neteautoDomain.

3. Wählen Sie unter neteautoDomain "Bereiche" aus.

   Die folgenden Bereiche werden angezeigt:

   **neteauto_ims_realm**

   Schützt die CA IdentityMinder-Umgebung.

   **neteauto_pub_realm**

   Ermöglicht den Support für öffentliche Aufgaben, wie etwa die Selbstregistrierung und die Aufgaben im Fall von vergessenen Kennwörtern.

4. Erstellen Sie in jedem der Bereiche eine Regel. Geben Sie die folgenden Details an:
   - Ressource: *
   - Aktionen: GET, POST

   Um die Verwaltung zu vereinfachen, nehmen Sie das NeteAuto-Design in den Regelnamen auf.

5. Erstellen Sie für die Domäne eine Antwort mit den folgenden Antwortattributen:
   - Attribut: WebAgent-HTTP-Header-Variable

     Dieses Attribut fügt einen neuen HTTP-Header zur Antwort hinzu.
   - Attributtyp: Statisch
   - Veränderlicher Name: Design

     Veränderlicher Wert: neteauto

6. Ändern Sie die Richtlinie, die CA IdentityMinder unter neteautoDomain erstellt hat. Geben Sie die folgenden Details an:
   - Benutzer
     - Für LDAP: Wählen Sie ou=People, ou=Employees oder ou=NeteAuto unter den verfügbaren Mitgliedern aus, und fügen Sie die jeweilige Auswahl zu den aktuellen Mitgliedern hinzu. Klicken Sie auf "OK".
     - Für relationale Datenbanken: Suchen Sie nach Benutzern, bei denen das ID-Attribut dem Wert "*" entspricht. Wählen Sie alle Benutzer unter den verfügbaren Mitgliedern aus, und fügen Sie diese zu den aktuellen Mitgliedern hinzu. Klicken Sie auf "OK".
   - Regeln (Rules):
     - Fügen Sie die Regeln hinzu, die Sie in Schritt 4 erstellt haben.
     - Klicken Sie für jede Regel auf "Vorgegebene Antwort". Verknüpfen Sie jede Regel mit der Antwort, die Sie in Schritt 5 erstellt haben.

**Hinweis:** Das neteauto-Design beruht auf der imcss-Konsole. Um das Design anzuzeigen, hängen Sie /imcss/index.jsp an die URL für die NeteAuto-CA IdentityMinder-Umgebung folgendermaßen an:

http://*hostname*/iam/im/neteauto/imcss/index.jsp

Der Zugriff auf die NeteAuto-CA IdentityMinder-Umgebung (siehe Seite 42) bietet vollständige Anweisungen für den Zugriff auf die NeteAuto-Umgebung.

## Verwenden Sie die entsprechende Funktion im Falle eines vergessenen Kennworts.

Führen Sie den folgenden Vorgang aus, um die Funktion für den Fall eines vergessenen Kennworts zu verwenden.

**Gehen Sie wie folgt vor:**

1. Geben Sie die folgende URL in einen Browser ein:

   `http://`*`hostname`*`/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   ***Hostname***

   Definiert den vollständig qualifizierten Domänennamen des Systems, in dem CA IdentityMinder betrieben wird.

2. Geben Sie die eindeutige Kennung für den selbst registrierten Benutzer ein, den Sie unter "Als neuer Benutzer registrieren" (siehe Seite 38) erstellt haben, und klicken Sie auf "Weiter".

3. Beantworten Sie bei jeder Aufforderung die Überprüfungsfrage. Die Antwort ist derjenige, die Sie während der Registrierung angegeben haben.

   **Hinweis**: Auf jede Frage ist die richtige Antwort erforderlich. Das Abbrechen der Aufgabe oder das Schließen des Browsers wird als fehlgeschlagener Versuch gewertet.

4. Klicken Sie auf "Senden".

   CA IdentityMinder fordert Sie auf, ein neues Kennwort bereitzustellen.

# Benutzerverwaltung

Die Benutzerverwaltung umfasst die folgenden Vorgänge:

- Zugreifen auf die NeteAuto-CA IdentityMinder-Umgebung
- Ändern eines Benutzers
- Zuweisen der Gruppen-Manager-Rolle
- Erstellen einer Gruppe
- Verwalten von selbst registrierten Benutzern

## Zugreifen auf die NeteAuto-CA IdentityMinder-Umgebung

Führen Sie den folgenden Vorgang aus, um auf die NeteAuto-CA IdentityMinder-Umgebung zuzugreifen.

**Gehen Sie wie folgt vor:**

1. Geben Sie die folgende URL in einen Browser ein:

   `http://`*`hostname`*`/iam/im/neteauto/imcss/index.jsp`

   **Hostname**

   Definiert den vollständig qualifizierten Domänennamen wie im folgenden Beispiel:

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp.

   **Hinweis:** Wenn Sie das NeteAuto-Design nicht konfiguriert haben, können Sie die folgende URL verwenden, um auf die NeteAuto-Umgebung zuzugreifen:

   http://*hostname*/iam/im/neteauto

2. Geben Sie im Anmeldefenster die folgenden Anmeldeinformationen ein:

   **Benutzername**

   SuperAdmin

   **Kennwort**

   test

## Einen Benutzer ändern

Führen Sie den folgenden Vorgang aus, um einen Benutzer zu ändern.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich als SuperAdmin an der NeteAuto-Umgebung mithilfe des Kennworttests an.
2. Benutzer auswählen, Benutzer verwalten, Benutzer ändern.

   Das Fenster "Benutzer auswählen" wird angezeigt.
3. Klicken Sie auf "Suchen".

   CA IdentityMinder zeigt eine Liste von Benutzern in der NeteAuto-Umgebung an.
4. Wählen Sie den NeteAuto-Administrator wie folgt aus:
   - Für LDAP-Verzeichnisse, NeteAuto-Administrator
   - Für relationale Datenbanken, NeteAuto Admin

   Klicken Sie auf "Auswählen". CA IdentityMinder zeigt das Profil für den NeteAuto-Administrator an.

5. Geben Sie "Manager" im Titel-Feld ein. Klicken Sie auf "Senden".

   CA IdentityMinder bestätigt die Aufgabenvorlage.

6. Klicken Sie auf "OK", um zum Hauptbildschirm zurückzukehren.

## Weisen Sie die Gruppen-Manager-Rolle zu.

Das Zuweisen einer Gruppenmanagerrolle ist notwendig. Führen Sie den folgenden Vorgang aus, um einen Gruppenmanager zuzuweisen.

**Gehen Sie wie folgt vor:**

1. Wählen Sie als SuperAdmin die Registerkarte für die Rollen und Aufgaben. Wählen Sie dann die Admin-Rollen aus, und ändern Sie diese.

2. Wählen Sie die Gruppen-Manager-Rolle aus, und klicken Sie auf "Auswählen".

   Das Profil für die Gruppen-Manager-Rolle wird angezeigt.

3. Klicken Sie auf die Registerkarte "Mitglieder" und anschließend auf "Hinzufügen" unter den Mitgliederrichtlinien.

   Das Fenster "Mitglieder-Richtlinie" wird angezeigt.

4. Klicken Sie unter der Mitgliederregel im Benutzer-Feld auf die Pfeil-nach-unten-Taste.

   Wählen Sie in der Drop-down-Liste den Eintrag <user-filter>.

   Das Benutzer-Feld ändert sich, damit Sie einen Filter für die Regel eingeben können.

5. Geben Sie eine Mitgliedschaftsregel wie folgt ein:

   a. Wählen Sie im ersten Feld den Titel aus der Drop-down-Liste aus.

   b. Vergewissern Sie sich, dass im zweiten Feld das Gleichheitszeichen (=) ausgewählt wird.

   c. Geben Sie "Manager" im dritten Feld ein.

6. Definieren Sie im Abschnitt der Umfangsregeln die Regeln für die Benutzer, Gruppen und Organisationen (sofern unterstützt) wie folgt:

   a. Klicken Sie im Benutzer-Feld auf die Pfeil-nach-unten-Taste, um eine Liste von Optionen anzusehen. Wählen Sie (alle) aus der Liste aus.

   b. Wiederholen Sie den Schritt "a" in den Feldern für die Gruppen und die Organisationen (sofern unterstützt).

   c. Lassen Sie das Feld für den Zugriff auf die Aufgaben leer.

7. Klicken Sie auf "OK".

   CA IdentityMinder zeigt die Mitgliederrichtlinie an, die Sie erstellt haben.

8. Klicken Sie auf "Senden".

   CA IdentityMinder bestätigt die Aufgabenvorlage.

9. Klicken Sie auf "OK", um zum Hauptbildschirm zurückzukehren.
10. Schließen Sie CA IdentityMinder.

## Erstellen Sie eine Gruppe.

Führen Sie den folgenden Vorgang aus, um eine Gruppe zu erstellen.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich wie folgt an CA IdentityMinder als NeteAuto-Administrator an:
   - Geben Sie bei LDAP-Verzeichnissen den Benutzernamen "NeteAuto-Administrator" ein, und führen Sie den Kennworttest durch.
   - Geben Sie bei relationalen Datenbanken den Benutzernamen "NeteAuto-Administrator" ein, und führen Sie den Kennworttest durch.

   Die Liste der Aufgaben, die der NeteAuto-Administrator ausführen kann, wird angezeigt. Da der NeteAuto-Administrator nur eine beschränkte Anzahl von Aufgaben ausführen kann, listet CA IdentityMinder die Aufgaben anstelle von Kategorien auf.
2. Klicken Sie auf "Gruppe erstellen".
3. Stellen Sie sicher, dass die Option zum Erstellen einer neuen Gruppe ausgewählt wird, und klicken Sie auf "OK".
4. Implementieren Sie einen der folgenden Schritte, der zu Ihrem Fall passt:
   - Wenn die NeteAuto-Umgebung Organisationen unterstützt:
     a. Klicken Sie im Feld für den Organisationsnamen auf das Ellipsensymbol (...), um die Organisation auszuwählen, in der CA IdentityMinder die Gruppe erstellt.
     b. Erweitern Sie NeteAuto unten im Fenster zum Auswählen der Organisation.
     c. Wählen Sie die Händler-Organisation aus.
   - Wenn die NeteAuto-Umgebung keine Organisationen unterstützt, fahren Sie mit dem nächsten Schritt fort.
5. Geben Sie die folgenden Informationen für die Gruppe ein:
   - Gruppenname: Händler-Administratoren
   - Gruppen-Beschreibung: Administratoren für NeteAuto-Verkaufsvertretung.
6. Klicken Sie auf die Registerkarte "Mitgliedschaft" und anschließend auf die Option zum Hinzufügen eines Benutzers.

   Das Fenster "Benutzer auswählen" wird angezeigt.

7. Klicken Sie auf "Suchen".
8. Markieren Sie den NeteAuto-Administrator, und klicken Sie auf "Auswählen".
9. Klicken Sie auf "Senden", um die Gruppe zu erstellen.

## Verwalten Sie die selbst registrierten Benutzer.

Führen Sie den folgenden Vorgang aus, wenn Sie selbst registrierte Benutzer verwalten möchten.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich mithilfe der folgenden Anmeldeinformationen am CA IdentityMinder als NeteAuto-Administrator an:
   - Für LDAP-Verzeichnisse:

     **Benutzername**

       NeteAuto-Administrator

     **Kennwort**

       test
   - Für relationale Datenbanken:

     **Benutzername**

       NeteAuto Admin

     **Kennwort**

       test

   Die Liste auf Aufgaben, die der NeteAuto-Administrator ausführen kann, wird auf der linken Seite der Benutzerkonsole angezeigt. Da der NeteAuto-Administrator nur eine beschränkte Anzahl von Aufgaben ausführen kann, listet CA IdentityMinder die Aufgaben anstelle von Kategorien auf.
2. Klicken Sie auf "Gruppe ändern".
3. Klicken Sie auf "Suchen".

   CA IdentityMinder zeigt eine Liste von Gruppen an.
4. Markieren Sie die Händler-Administratoren, und klicken Sie auf "Auswählen".
5. Klicken Sie auf die Registerkarte "Mitgliedschaft" und anschließend auf die Option zum Hinzufügen eines Benutzers.

   Das Fenster "Benutzer auswählen" wird angezeigt.
6. Klicken Sie auf "Suchen".
7. Wählen Sie im Benutzer-Suchfenster den Benutzer, den Sie unter "Als neuen Benutzer registrieren" (siehe Seite 38) eingegeben haben. Klicken Sie auf "Auswählen".

8. Klicken Sie auf "Senden".

   CA IdentityMinder bestätigt die Aufgabenvorlage.

9. Klicken Sie auf "OK", um zum Hauptbildschirm zurückzukehren.

Um zu bestätigen, dass der Benutzer ein Mitglied der erstellten Gruppe ist, verwenden Sie die Aufgabe zum Anzeigen von Gruppen.

# So werden zusätzliche Funktionen konfiguriert

Sobald Sie das NeteAuto-Beispiel installiert und den Umgang mit der grundlegenden CA IdentityMinder-Funktionalität geübt haben, verwenden Sie die NeteAuto-Umgebung, um den Umgang mit zusätzlichen CA IdentityMinder-Funktionen einschließlich E-Mail-Benachrichtigungen und Workflow zu üben und diese zu testen.

**Hinweis**: Weitere Informationen zu diesen Funktionen finden Sie im *Administrationshandbuch*.

# Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen

Folgende Zeichen oder Zeichenfolgen darf ein globaler Benutzername nicht enthalten, wenn der Benutzer sich auf dem SiteMinder-Richtlinienserver anmelden können soll:

&<br>
*<br>
:<br>
()

**Behelfslösung**

Vermeiden Sie die Verwendung dieser Zeichen im globalen Benutzernamen.

# Kapitel 3: Verwaltung des LDAP-Benutzerspeichers

Dieses Kapitel enthält folgende Themen:

CA IdentityMinder-Verzeichnisse (siehe Seite 47)
So erstellen Sie ein CA IdentityMinder-Verzeichnis (siehe Seite 48)
Verzeichnisstruktur (siehe Seite 48)
Verzeichniskonfigurationsdatei (siehe Seite 50)
So wählen Sie eine Verzeichnis-Konfigurations-Vorlage aus (siehe Seite 51)
So wird ein Benutzerverzeichnis für CA IdentityMinder beschrieben (siehe Seite 53)
Verbindung zum Benutzerverzeichnis (siehe Seite 54)
Verzeichnissuchparameter (siehe Seite 58)
Beschreibungen der über Benutzer, Gruppe und Organisation verwalteten Objekte (siehe Seite 60)
Bekannte Attribute für einen LDAP-Benutzerspeicher (siehe Seite 79)
Beschreiben der Benutzerverzeichnisstruktur (siehe Seite 87)
So konfigurieren Sie Gruppen (siehe Seite 88)
Validierungsregeln (siehe Seite 91)
Zusätzliche Eigenschaften des CA IdentityMinder-Verzeichnisses (siehe Seite 92)
So verbessern Sie die Leistung von Verzeichnissuchen (siehe Seite 96)

## CA IdentityMinder-Verzeichnisse

Ein *CA IdentityMinder-Verzeichnis* beschreibt, wie Objekte wie etwa Benutzer, Gruppen und Organisationen im Benutzerverzeichnis gespeichert werden und wie diese in CA IdentityMinder dargestellt werden. Ein CA IdentityMinder-Verzeichnis ist einer oder mehreren CA IdentityMinder-Umgebungen zugeordnet.

# So erstellen Sie ein CA IdentityMinder-Verzeichnis

Beim Erstellen eines CA IdentityMinder-Verzeichnisses für einen LDAP-Benutzerspeicher sind die folgenden Schritte durchzuführen:

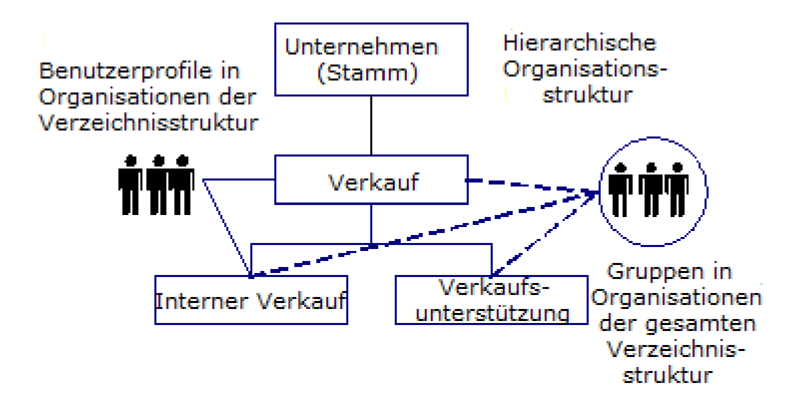
1. Festlegen der Verzeichnisstruktur.
2. Beschreiben der Objekte im Benutzerspeicher durch Ändern einer Verzeichniskonfigurationsdatei (directory.xml) (siehe Seite 53).
3. Importieren der Verzeichniskonfigurationsdatei und Erstellen des Verzeichnisses (siehe Seite 157).

**Hinweis:** Überprüfen Sie bei der Verwendung von SiteMinder, dass Sie vor dem Erstellen des CA IdentityMinder-Verzeichnisses das Richtlinienspeicherschema angewendet haben. Weitere Informationen zu spezifischen Richtlinienspeicherschemen und darüber, wie diese anzuwenden sind, können Sie dem *Installationshandbuch* entnehmen.

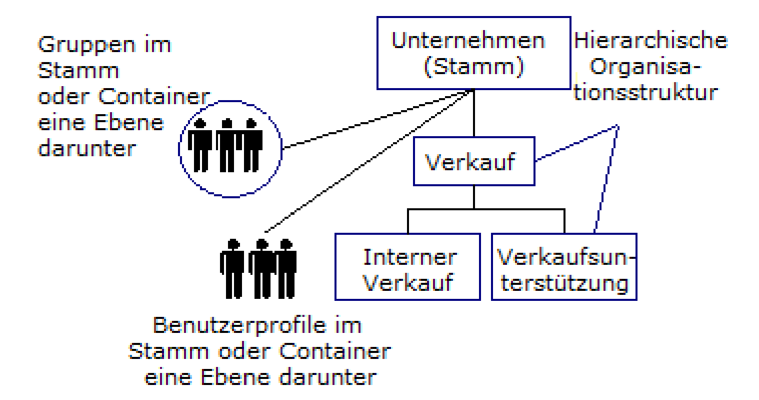
## Verzeichnisstruktur

CA IdentityMinder unterstützt die folgenden Verzeichnisstrukturen:

- Hierarchisch - Enthält eine übergeordnete Organisation (Stamm) und Unterorganisationen. Die Unterorganisationen können ebenfalls Unterorganisationen besitzen, was zu einer Multiebenen-Struktur führt. Dies lässt sich in der folgenden Abbildung erkennen:

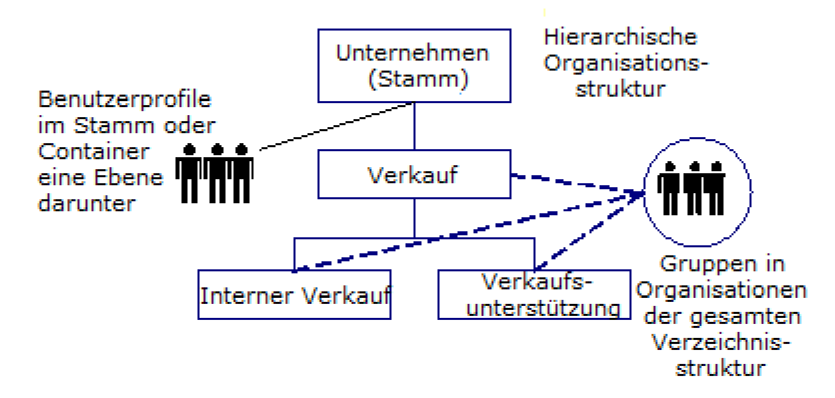


- Flach - Benutzer und Gruppen werden im Suchstamm oder in einem Container eine Ebene unterhalb des Suchstamms gespeichert. Organisationen besitzen eine hierarchische Struktur, wie in der folgenden Abbildung einer flachen Verzeichnisstruktur angezeigt wird:



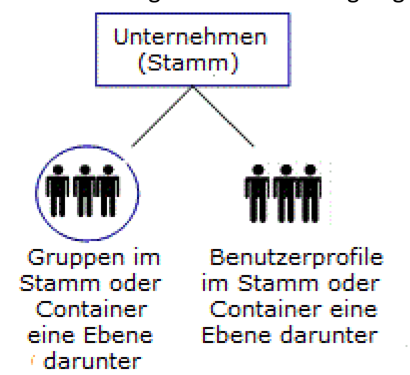

Um die Benutzerverwaltung und Delegation in flachen Verzeichnisstrukturen zu erleichtern, gehören Benutzer und Gruppen zu logischen Organisationen. Die logische Organisation wird als ein Attribut in Benutzer- und Gruppenprofilen gespeichert.

- Flache Benutzer - Organisationen und Gruppen werden hierarchisch gespeichert. Benutzer werden jedoch im Suchstamm oder in einem Container eine Ebene unterhalb des Suchstamms gespeichert. Die Darstellung der Verzeichnisstruktur eines flachen Benutzers wird im folgenden Diagramm angezeigt:




In den Verzeichnisstrukturen eines flachen Benutzers gehören Benutzer zu logischen Organisationen. Die logische Organisation eines Benutzers wird als Attribut in einem Benutzerprofil gespeichert.

- Keine Organisationen - Das Verzeichnis schließt keine Organisationen ein. Benutzer und Gruppen werden im Suchstamm oder in einem Container eine Ebene unterhalb des Suchstamms gespeichert. Die Verzeichnisstruktur zu "Keine Organisationen" wird in der folgenden Darstellung angezeigt:




**Hinweis:** Ein Verzeichnis kann mehr als einen Strukturtyp enthalten. Beispiel: Benutzerprofile können in einer flachen Struktur in einem Teil des Verzeichnisses und hierarchisch in einem anderen gespeichert werden. Um eine hybride Verzeichnisstruktur zu unterstützen, erstellen Sie mehrere CA IdentityMinder-Umgebungen.

# Verzeichniskonfigurationsdatei

Um CA IdentityMinder die Struktur eines Benutzerverzeichnisses zu beschreiben, erstellen Sie eine Verzeichniskonfigurationsdatei.

Die Verzeichniskonfigurationsdatei enthält einen oder mehrere der folgenden Abschnitte:

**Informationen zum CA IdentityMinder-Verzeichnis**

Enthält Informationen über das CA IdentityMinder-Verzeichnis.

**Hinweis:** Ändern Sie keine Information in diesem Abschnitt. CA IdentityMinder fordert Sie auf, diese Information anzugeben, wenn Sie ein CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen.

**Attributvalidierung**

Definiert die Validierungsregeln, die auf das CA IdentityMinder-Verzeichnis angewandt werden.

**Informationen zum Anbieter**

Beschreibt den Benutzerspeicher, den CA IdentityMinder verwaltet.

**Informationen zur Verzeichnissuche**

Ermöglicht Ihnen, anzugeben, wie CA IdentityMinder den Benutzerspeicher durchsucht.

**Benutzerobjekt**

Beschreibt, wie Benutzer im Benutzerspeicher gespeichert und wie sie in CA IdentityMinder dargestellt werden.

**Gruppenobjekt**

Beschreibt, wie Gruppen im Benutzerspeicher gespeichert und wie sie in CA IdentityMinder dargestellt werden.

**Organisationsobjekt**

Beschreibt, wie Organisationen gespeichert und wie sie in CA IdentityMinder dargestellt werden. Das Organisationsobjekt stellt nur dann Details bereit, wenn der Benutzerspeicher Organisationen enthält.

**Self-Subscribing-Objekt**

Konfiguriert die Unterstützung für Gruppen, denen Self-Service-Benutzer beitreten können.

**Verhalten der Verzeichnis-Gruppen**

Gibt an, ob das CA IdentityMinder-Verzeichnis dynamische und verschachtelte Gruppen unterstützt.

Um eine Verzeichniskonfigurationsdatei zu erstellen, ändern Sie eine Konfigurationsvorlage.

# So wählen Sie eine Verzeichnis-Konfigurations-Vorlage aus

CA IdentityMinder liefert Verzeichniskonfigurationsvorlagen, die unterschiedliche Verzeichnistypen und -strukturen unterstützen. Um ein CA IdentityMinder-Verzeichnis zu erstellen, ändern Sie die Vorlage, die Ihrer Verzeichnisstruktur am nächsten kommt.

Die in der folgenden Tabelle beschriebenen Vorlagen werden mit den Administrations-Tools installiert:

*admin_tools*\directoryTemplates*directory_type*\

Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Die Typen von Verzeichnissen und die entsprechenden Konfigurationsvorlagen werden in der folgenden Tabelle angezeigt:

| Verzeichnistyp | Vorlage |
|---|---|
| Active Directory (ADSI) LDAP-Verzeichnis mit einer hierarchischen Struktur | ActiveDirectory\directory.xml |
| Microsoft ADAM-Verzeichnis mit einer hierarchischen Struktur | ADAM\directory.xml |
| IBM Directory Server-Verzeichnis mit einer hierarchischen Struktur | IBMDirectoryServer\directory.xml |
| Novell eDirectory-Benutzerverzeichnis mit einer hierarchischen Struktur | eDirectory\directory.xml |
| Oracle Internet Directory mit einer hierarchischen Struktur | OracleInternetDirectory\directory.xml |
| Sun Java-System (SunOne oder iPlanet) LDAP-Verzeichnis mit einer hierarchischen Struktur | IPlanetHierarchical\directory.xml |
| Sun Java-System (SunOne oder iPlanet) LDAP-Verzeichnis mit einer flachen Struktur | IPlanetFlat\directory.xml |
| Sun Java-System (SunOne oder iPlanet) LDAP-Verzeichnis, das keine Organisationen enthält. | IPlanetNoOrganizations\directory.xml |
| CA Directory-Benutzerspeicher mit einer hierarchischen Struktur | eTrustDirectory\directory.xml |
| Bereitstellungsverzeichnis<br>Diese Vorlage konfiguriert das Bereitstellungsverzeichnis (Provisioning-Verzeichnis) für eine CA IdentityMinder-Umgebung.<br>**Hinweis:** Sie können diese Konfigurationsvorlage wie installiert verwenden. Sie müssen diese Vorlage nicht ändern. | ProvisioningServer\directory.xml |

| Verzeichnistyp | Vorlage |
|---|---|
| Benutzerdefiniertes Verzeichnis | Verwenden Sie die Vorlage, die Ihrem Verzeichnis am nächsten kommt. |

Kopieren Sie die Konfigurationsvorlage in ein neues Verzeichnis, oder speichern Sie sie unter einem anderen Namen, damit sie nicht überschrieben wird.

# So wird ein Benutzerverzeichnis für CA IdentityMinder beschrieben

Um ein Verzeichnis zu verwalten, muss CA IdentityMinder die Struktur und den Inhalt eines Verzeichnisses verstehen. Um das Verzeichnis für CA IdentityMinder zu beschreiben, ändern Sie die Verzeichniskonfigurationsdatei (directory.xml) im entsprechenden Vorlagenverzeichnis.

Die Verzeichniskonfigurationsdatei weist die folgenden wichtigen Konventionen auf:

- ## - Kennzeichnet erforderliche Werte.

  Um sämtliche erforderlichen Information anzugeben, müssen Sie alle doppelten Rautenzeichen (##) ausfindig machen und diese durch entsprechende Werte ersetzen. Beispiel: ##DISABLED_STATE zeigt an, dass Sie ein Attribut bereitstellen müssen, um den Kontostatus eines Benutzers zu speichern.
- @ - Kennzeichnet Werte, die von CA IdentityMinder ausgefüllt werden. Diese Werte dürfen in der Verzeichniskonfigurationsdatei nicht geändert werden. CA IdentityMinder fordert Sie beim Import der Verzeichniskonfigurationsdatei auf, diese Werte anzugeben.

Bevor Sie die Verzeichniskonfigurationsdatei ändern, benötigen Sie die folgenden Informationen:

- LDAP-Objektklassen für die Benutzer-, Gruppen- und Organisationsobjekte
- Liste von Attributen in Benutzer-, Gruppen- und Organisationsprofilen

## So wird die Verzeichniskonfigurationsdatei geändert

Führen Sie die folgenden Schritte aus, um die Verzeichniskonfigurationsdatei zu ändern.

**Hinweis:** Schritte, die erforderlich sind, werden entsprechend aufgeführt.

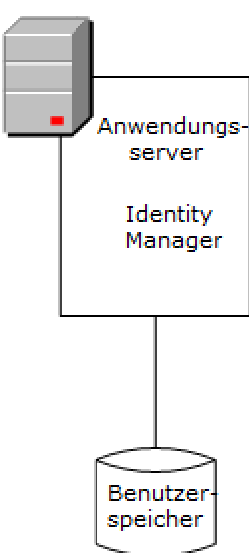
1. Begrenzen Sie den Umfang der Suchergebnisse (siehe Seite 58).
2. Ändern Sie die durch Standardbenutzer, Organisation oder Gruppe verwalteten Objekte.

3. Ändern Sie die Standardattributbeschreibungen.
4. Ändern Sie bekannte Attribute (siehe Seite 79). (erforderlich)

   Bekannte Attribute kennzeichnen besondere Attribute, wie das Kennwortattribut in CA IdentityMinder.
5. Konfigurieren Sie CA IdentityMinder für Ihre Verzeichnisstruktur (siehe Seite 87) (erforderlich).
6. Ermöglicht es Benutzern, sich an Gruppen anzumelden (siehe Seite 88).

# Verbindung zum Benutzerverzeichnis

CA IdentityMinder stellt eine Verbindung zu einem Benutzerverzeichnis her, um Informationen, wie etwa zu Benutzer, Gruppe oder auch organisatorische Information, wie in der folgenden Darstellung angezeigt zu speichern:




Ein neues Verzeichnis oder eine neue Datenbank sind nicht erforderlich. Allerdings müssen das bestehende Verzeichnis oder die Datenbank auf einem System vorhanden sein, das einen vollständig qualifizierten Domänennamen besitzt (FQDN).

Eine Liste der unterstützten Verzeichnis- und Datenbanktypen finden Sie über die CA IdentityMinder-Support-Matrix auf der CA Support-Website.

Sie konfigurieren eine Verbindung zum Benutzerspeicher, wenn Sie ein CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen.

Wenn Sie die Verzeichniskonfiguration exportieren, nachdem Sie ein CA IdentityMinder-Verzeichnis erstellt haben, werden die Verbindungsinformationen zum Benutzerverzeichnis im Anbieter-Element der Verzeichniskonfigurationsdatei angezeigt.

# Provider-Element

Konfigurationsinformationen werden im Anbieter-Element und dessen Unterelementen in der directory.xml-Datei gespeichert.

**Hinweis:** Wenn Sie ein CA IdentityMinder-Verzeichnis erstellen, müssen Sie keine Verzeichnisverbindungsinformationen in der Datei "directory.xml" angeben. Die Verbindungsinformationen werden im Assistenten für CA IdentityMinder-Verzeichnisse in der Management-Konsole angegeben. Ändern Sie das Provider-Element nur für Aktualisierungen.

Das Provider-Element beinhaltet die folgenden Unterelemente:

**LDAP**

Beschreibt das Benutzerverzeichnis, zu dem Sie eine Verbindung herstellen.

**Anmeldeinformationen**

Gibt den Benutzernamen und das Kennwort für den Zugriff auf den LDAP-Benutzerspeicher an.

**Verbindung**

Gibt den Hostnamen und den Port für den Computer an, auf dem sich der Benutzerspeicher befindet.

**Bereitstellungsdomäne**

Definiert die Provisioning-Domäne, die durch CA IdentityMinder verwaltet wird (ausschließlich für Provisioning-Benutzer).

Ein abgeschlossenes Anbieter-Element entspricht dem folgenden Code:

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

Das Anbieter-Element umfasst die folgenden Parameter:

**type**

Gibt den Typ der Datenbank an. Geben Sie LDAP (Standard) für alle LDAP-Benutzerspeicher an.

**userdirectory**

Gibt den Namen der Benutzerverzeichnisverbindung an.

**Hinweis:** Geben Sie keinen Namen für die Benutzerverzeichnisverbindung in der Datei "directory.xml" an. CA IdentityMinder fordert Sie auf, den Namen anzugeben, wenn Sie das CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen.

**Hinweis:** Die Parameter sind optional.

## LDAP-Unterelement

Das LDAP-Unterelement enthält die folgenden Parameter:

**searchroot**

Gibt den Speicherort in einem LDAP-Verzeichnis an, das als Ausgangspunkt für das Verzeichnis dient. Üblicherweise ist dies eine Organisation (O) oder eine Organisationseinheit (OU).

**sicher**

Erzwingt eine Secure Sockets Layer (SSL) Verbindung zum LDAP-Benutzerverzeichnis wie folgt:

- True - CA IdentityMinder verwendet eine sichere Verbindung.
- False - CA IdentityMinder stellt ohne SSL (Standard) eine Verbindung zum Benutzerverzeichnis her.

**Hinweis:** Die Parameter sind optional.

## Anmeldeinformationen-Unterelement

Um eine Verbindung zu einem LDAP-Verzeichnis herzustellen, muss CA IdentityMinder gültige Anmeldeinformationen bereitstellen. Die Anmeldeinformationen werden in dem Anmeldeinformationen-Unterelement definiert, das dem folgenden Code entspricht:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Sofern Sie kein Kennwort in den Anmeldeinformationen angeben, verlangt das Unterelement nach dem Kennwort, wenn Sie das CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen.

**Hinweis:** Es wird empfohlen, das Kennwort in der Management-Konsole anzugeben.

Wenn Sie das Kennwort in der Management-Konsole angeben, wird es von CA IdentityMinder verschlüsselt. Andernfalls sollten Sie das Kennwort mit dem Kennwort-Tool, das zusammen mit CA IdentityMinder installiert wird, verschlüsseln, sodass dieses nicht als unverschlüsselter Text angezeigt wird.

**Hinweis:** Sie können nur einen Satz von Anmeldeinformationen angeben. Wenn Sie mehrere Verzeichnisse definieren, wie im Verbindungs-Unterelement beschrieben, müssen die von Ihnen angegebenen Anmeldeinformationen für alle Verzeichnisse gelten.

Das Anmeldeinformationen-Unterelement enthält die folgenden Parameter:

**user**

Gibt die Anmelde-ID für ein Konto an, das auf das Verzeichnis zugreifen kann.

Bei Provisioning-Benutzern muss das Benutzerkonto, das Sie angeben, das Domänenadministrator-Profil oder ein gleichwertiges Set von Berechtigungen im Provisioning-Server besitzen.

**Hinweis:** Geben Sie keinen Wert für den Benutzerparameter in der directory.xml-Datei an. CA IdentityMinder fordert Sie beim Erstellen des CA IdentityMinder-Verzeichnisses in der Management-Konsole zur Eingabe der Anmelde-ID auf.

**cleartext**

Legt fest, ob das Kennwort wie folgt im Fließtext in der directory.xml-Datei angezeigt wird:

- True - Das Kennwort wird als unverschlüsselter Text angezeigt.
- False - Das Kennwort wird verschlüsselt (Standardeinstellung).

**Hinweis:** Die Parameter sind optional.

## Verbindungs-Unterelement

Das Verbindungs-Unterelement beschreibt den Speicherort des Benutzerspeichers, den CA IdentityMinder verwaltet. Dieses Unterelement enthält die folgenden Parameter:

**Host**

Gibt den Hostnamen oder die IP-Adresse des Systems an, in dem sich das Benutzerverzeichnis befindet.

**Hinweis:** Wenn das verbundene System eine IPv6-Adresse aufweist, fügen Sie die IP-Adresse innerhalb der Klammern ([ ]) wie folgt bei:

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

**port**

Gibt die Port-Nummer für das Benutzerverzeichnis an.

**Failover**

Gibt den Hostnamen und die IP-Adresse des Systems an, in dem redundante Benutzerspeicher vorhanden sind. Dies ist für den Fall vorgesehen, dass das Primärsystem nicht verfügbar ist. Wenn das Primärsystem wieder verfügbar ist, kann das Failover-System wieder verwendet werden. Um zur Verwendung des Primärsystems zurückzukehren, starten Sie das sekundäre System neu. Wenn mehrere Server aufgelistet sind, versucht CA IdentityMinder, eine Verbindung zu den Systemen in der aufgelisteten Reihenfolge herzustellen.

Geben Sie den Hostnamen und die IP-Adresse im Failover-Attribut in einer *unterteilten* Liste wie folgt an:

failover="IPaddress:port IPaddress:port"

Beispiel:

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389123.456.789.003:20389"/>

**Hinweis:** Port 20389 ist der Standard-Port für den Provisioning-Server.

**Hinweis:** Die Parameter sind optional.

## Provisioning-Unterelement

Wenn die CA IdentityMinder-Umgebung eine Bereitstellung umfasst, definieren Sie die Provisioning-Domäne folgendermaßen:

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

Das Provisioning-Unterelement enthält den folgenden Parameter:

**domain**

Gibt den Namen der Provisioning-Domäne an, die durch CA IdentityMinder verwaltet wird.

Wenn Sie das CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen, werden Sie nach dem Domänennamen gefragt. Überprüfen Sie, dass Sie einen Wert für den Domänenparameter in der Verzeichniskonfigurationsdatei (directory.xml) angeben.

# Verzeichnissuchparameter

Sie können die folgenden Suchparameter im DirectorySearch-Element festlegen:

**maxrows**

Gibt die maximale Zahl an Objekten an, die CA IdentityMinder beim Suchen in einem Benutzerverzeichnis zurückgeben kann. Wenn die Anzahl an Objekten das Limit überschreitet, wird ein Fehler angezeigt.

Durch Festlegen eines Wertes für den Maxrows-Parameter, können Sie die Einstellungen im LDAP-Verzeichnis überschreiben, welche die Suchergebnisse beschränken. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Hinweis:** Der Maxrows-Parameter beschränkt nicht die Anzahl an Objekten, die in einem CA IdentityMinder-Aufgabenfenster angezeigt werden. Um die Anzeigeeinstellungen zu konfigurieren, ändern Sie die Listenfensterdefinition in der CA IdentityMinder-Benutzerkonsole. Weitere Anweisungen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**maxpagesize**

Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

Beachten Sie beim Spezifizieren von maxpagesize die folgenden Aspekte:

- Um die Option "maxpagesize" zu verwenden, muss der von CA IdentityMinder verwaltete Benutzerspeicher Paging unterstützen. Einige Benutzerspeichertypen erfordern jedoch zusätzliche Konfigurationsschritte, damit sie Paging unterstützen. Weitere Informationen können Sie dem Abschnitt "So verbessern Sie die Leistung bei großen Suchen" (siehe Seite 97) entnehmen.
- Wenn der Benutzerspeicher kein Paging unterstützt und auch ein Wert für "maxrows" angegeben wird, verwendet CA IdentityMinder ausschließlich den maxrows-Wert, um die Suchgröße zu steuern.

**Verbindungszeitlimit**

Gibt die maximale Anzahl an Sekunden an, die CA IdentityMinder in einem Verzeichnis sucht, bevor die Suche beendet wird.

**Hinweis:** Das DirectorySearch-Element ist optional. Wenn das Verzeichnis allerdings Paging (siehe Seite 97) unterstützt, wird empfohlen, das DirectorySearch-Element anzugeben.

**Weitere Informationen:**

So verbessern Sie die Leistung von Verzeichnissuchen (siehe Seite 96)
So verbessern Sie die Leistung von großen Suchen (siehe Seite 97)

# Beschreibungen der über Benutzer, Gruppe und Organisation verwalteten Objekte

In einem CA IdentityMinder verwalten Sie die folgenden Typen von Objekten, die den Eingaben in einem Benutzerverzeichnis entsprechen:

**Benutzer**

Diese repräsentieren die Benutzer in einem Unternehmen. Ein Benutzer gehört zu einer einzelnen Organisation.

**Gruppen**

Diese repräsentieren Verbindungen von Benutzern, die etwas gemeinsam haben.

**Organisationen**

Diese repräsentieren Business Units. Organisationen enthalten Details zu Benutzern, Gruppen oder anderen Organisationen.

Eine Objektbeschreibung enthält die folgenden Informationen:

- Informationen zum Objekt (siehe Seite 118), wie etwa zur LDAP-Objektklasse oder zum Container, in dem Objekte gespeichert werden.
- Die Attribute, in denen Informationen zu einem Eintrag gespeichert sind (siehe Seite 123). Zum Beispiel ist im Attribut "pager" eine Pagernummer gespeichert.

**Hinweis:** Eine CA IdentityMinder-Umgebung unterstützt nur einen Typ von Benutzer, Gruppe oder Organisationsobjekt. Zum Beispiel weisen alle Benutzerobjekte die gleiche Objektklasse auf.

## Beschreibung von verwalteten Objekten

Ein verwaltetes Objekt wird durch das Angeben der Objektinformation in den Benutzerobjekt-, Gruppenobjekt- und Organisationsobjekt-Abschnitten der Verzeichniskonfigurationsdatei beschrieben.

**Hinweis:** Wenn die Konfigurationsvorlage (directory.xml-Datei) verwendet wird, ist der Organisationsobjekt-Abschnitt für jene Benutzerverzeichnisse nicht verfügbar, die keine Organisationen unterstützen.

Jeder dieser Abschnitte enthält ImsManagedObject-Elemente, wie im folgenden Beispiel dargestellt:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

Optional kann das ImsManagedObject-Element ein Container-Element enthalten, wie im folgenden Beispiel dargestellt:

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

## Angeben von Objektinformationen

Objektinformationen werden angegeben, indem Sie Werte für verschiedene Parameter festlegen.

**Gehen Sie wie folgt vor:**

1. Machen Sie das ImsManagedObject-Element im Benutzerobjekt-, Organisationsobjekt- oder Gruppenobjekt-Abschnitt ausfindig.
2. Geben Sie Werte für die folgenden Parameter an:

   **name**

   Gibt einen eindeutigen Namen für das verwaltete Objekt an.

   **Hinweis:** Dieser Parameter ist erforderlich.

   **Beschreibung**

   Enthält eine Beschreibung des verwalteten Objekts.

   **objectclass**

   Gibt den Namen der LDAP-Objektklasse für den Objekttyp (Benutzer, Gruppe oder Organisation) an. Die Objektklasse bestimmt die Liste der verfügbaren Attribute für ein Objekt.

   Wenn Attribute aus mehreren Objektklassen für einen Objekttyp gelten, listen Sie die Objektklassen in einer durch Kommas abgegrenzten Liste auf. Wenn ein Objekt zum Beispiel Attribute aus den Person-, Organizationalperson- oder Inetorgperson-Objektklassen enthält, fügen Sie diese Objektklassen wie folgt hinzu:

   objectclass="top,person,organizationalperson,inetorgperson"

   Jedes LDAP-Verzeichnis enthält ein Set von vordefinierten Objektklassen. In der Verzeichnisserver-Dokumentation finden Sie Informationen zu vordefinierten Objektklassen.

   **Hinweis:** Dieser Parameter ist erforderlich.

**objecttype**

Gibt den Typ des verwalteten Objekts an. Die folgenden Werte sind gültig:

- User
- Organisation
- Gruppe

**Hinweis:** Dieser Parameter ist erforderlich.

**maxrows**

Gibt die maximale Zahl an Objekten an, die CA IdentityMinder beim Suchen in einem Benutzerverzeichnis zurückgeben kann. Wenn die Anzahl an Objekten das Limit überschreitet, wird ein Fehler angezeigt.

Durch Festlegen eines Wertes für den Maxrows-Parameter, können Sie die Einstellungen im LDAP-Verzeichnis überschreiben, welche die Suchergebnisse beschränken. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Hinweis:** Der Maxrows-Parameter beschränkt nicht die Anzahl an Objekten, die in einem CA IdentityMinder-Aufgabenfenster angezeigt werden. Um die Anzeigeeinstellungen zu konfigurieren, ändern Sie die Listenfensterdefinition in der CA IdentityMinder-Benutzerkonsole. Weitere Anweisungen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**maxpagesize**

Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

Beachten Sie die folgenden Aspekte beim Angeben der Suchseiten-Größe:

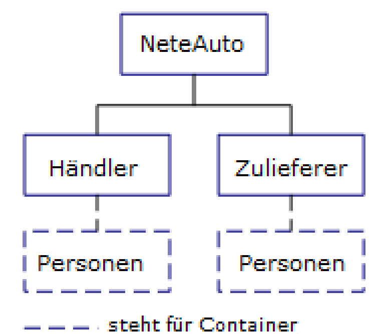
- Damit Sie die Option zur Festlegung der Seitengröße von Suchen verwenden können, muss der von CA IdentityMinder verwaltete Benutzerspeicher Paging unterstützen. Einige Benutzerspeichertypen erfordern jedoch zusätzliche Konfigurationsschritte, damit sie Paging unterstützen. Weitere Informationen können Sie dem Abschnitt "So verbessern Sie die Suchleistung" (siehe Seite 97) entnehmen.
- Wenn der Benutzerspeicher kein Paging unterstützt und auch ein Wert für "maxrows" angegeben wird, verwendet CA IdentityMinder ausschließlich den maxrows-Wert, um die Suchgröße zu steuern.

3. Stellen Sie optional die Container-Informationen bereit.

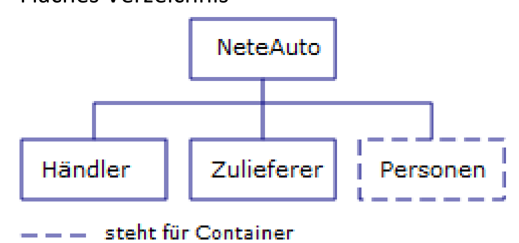
## Container

Um die Verwaltung zu vereinfachen, können Sie Objekte eines bestimmten Typs in einem Container gruppieren. Wenn Sie einen Container in der Verzeichniskonfigurationsdatei angeben, verwaltet CA IdentityMinder ausschließlich Eingaben in dem Container. Wenn Sie zum Beispiel einen Benutzer-Container namens "People" angeben, verwaltet CA IdentityMinder die Benutzer im People-Container, wie in den folgenden Abbildungen dargestellt:

- Hierarchisches Verzeichnis




- Flaches Verzeichnis




In diesen Beispielen liegen alle Benutzer in den People-Containern vor.

Wenn Sie einen Container angeben, müssen Sie die folgenden Punkte beachten:

- Wenn kein Container in einer Organisation vorhanden ist, erstellt CA IdentityMinder den Container, sobald die erste Eingabe hinzugefügt wird. Beim einem hierarchischen Verzeichnis erstellt CA IdentityMinder den Container in der Organisation, in der die Eingabe hinzugefügt wird. Bei flachen Verzeichnissen und bei jenen Verzeichnissen, die keine Organisationen unterstützen, erstellt CA IdentityMinder den Container unter dem Suchstamm, den Sie angeben, wenn Sie das CA IdentityMinder-Verzeichnis erstellen.
- CA IdentityMinder ignoriert Eingaben, die nicht im angegebenen Container vorhanden sind. Wenn Sie zum Beispiel den People-Container angeben, können Sie keine Benutzer verwalten, die außerhalb des People-Containers vorhanden sind.

  **Hinweis:** Um Benutzer zu verwalten, die nicht im angegebenen Container vorhanden sind, können Sie eine weitere CA IdentityMinder-Umgebung erstellen.

## Container und bekannte Attribute

Bekannte Attribute sind Attribute, denen in CA IdentityMinder eine besondere Bedeutung zukommt. Wenn CA IdentityMinder einen Benutzerspeicher einschließlich Containern verwaltet, identifizieren die folgenden bekannten Attribute die Informationen zu den Containern:

**%ORG_MEMBERSHIP%**

Identifiziert das Attribut, das den vollständigen Namen (DN) des Containers speichert.

Zum Beispiel entspricht der vollständige Name Folgendem:

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

**%ORG_MEMBERSHIP_NAME%**

Identifiziert das Attribut, das den benutzerfreundlichen Namen des Attributs speichert.

So lautet zum Beispiel der benutzerfreundliche Name des Containers im vorigen Beispiel "People".

Diese bekannten Attribute werden folgendermaßen in den Attributbeschreibungen in den Benutzerobjekt- und Gruppenobjekt-Abschnitten der directory.xml-Datei angezeigt:

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Für hierarchische Benutzerspeicher-Strukturen werden die physicalname-Parameter und die bekannten Parameter wie folgt zum bekannten Attribut zugeordnet:

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Das Beispiel zeigt an, dass CA IdentityMinder automatisch den Container-DN und den benutzerfreundlichen Namen aus anderen Informationen in der directory.xml-Datei ableitet.

Stellen Sie für flache Benutzerspeicher-Strukturen die physischen Attributnamen bereit.

**Hinweis:** Entsprechende Anweisungen finden Sie im Abschnitt "So beschreiben Sie eine flache Benutzerverzeichnis-Struktur" (siehe Seite 87).

## Geben Sie einen Benutzer- oder Gruppen-Container an.

Führen Sie den folgenden Vorgang aus, um einen Benutzer- oder Gruppen-Container anzugeben.

**Gehen Sie wie folgt vor:**

1. Machen Sie das Container-Element im Benutzerobjekt- oder Gruppenobjekt-Abschnitt ausfindig.
2. Geben Sie Werte für die folgenden Parameter an:

   **objectclass**

   Legt die LDAP-Objektklasse des Containers fest, in dem die Objekte eines bestimmten Typs erstellt werden. Zum Beispiel ist der Standardwert für den Benutzercontainer "top,organizationalUnit", was anzeigt, dass Benutzer in LDAP-Organisationseinheiten (ou) erstellt werden.

   Wenn Sie dynamische oder verschachtelte Gruppen verwalten, müssen Sie sicherstellen, dass Sie eine Objektklasse angeben, die diese Gruppentypen unterstützt (siehe Seite 89).

   **Hinweis:** Dieser Parameter ist erforderlich.

   **Attribut**

   Gibt das Attribut an, das den Containernamen, zum Beispiel "ou", speichert.

   Das Attribut wird paarweise mit dem Wert angeordnet, um das relative DN des Containers zu bilden, wie im folgenden Beispiel dargestellt:

   ou=People

   **Hinweis:** Dieser Parameter ist erforderlich.

   **value**

   Gibt den Namen des Containers an.

   **Hinweis:** Dieser Parameter ist erforderlich.

**Hinweis:** Sie können keine Container für Organisationen angeben.

## Attributbeschreibungen

Ein Attribut speichert Information zu einer Eingabe, wie etwa eine Telefonnummer oder Adresse. Ein Eingabeattribut bestimmt das entsprechende Profil.

In der Verzeichniskonfigurationsdatei werden Attribute in ImsManagedObjectAttr-Elementen beschrieben. In den Benutzerobjekt-, Gruppenobjekt- und Organisationsobjekt-Abschnitten der Verzeichniskonfigurationsdatei können Sie die folgenden Aktionen durchführen:

- Ändern Sie die Standardattributbeschreibungen, um die Attribute in Ihrem Benutzerspeicher zu beschreiben.
- Erstellen Sie neue Attributbeschreibungen, indem Sie eine vorhandene Beschreibung kopieren und Werte nach Bedarf ändern.

Für jedes Attribut in Benutzer-, Gruppen- und Organisationsprofilen liegt ein ImsManagedObjectAttr-Element vor. So wird zum Beispiel ein ImsManagedObjectAttr-Element als Benutzer-ID bezeichnet.

Ein ImsManagedObjectAttr-Element entspricht dem folgenden Code:

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User
ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%"
maxlength="0" />
```

ImsManagedObjectAttr weist die folgenden Parameter auf:

**physicalname**

Dieser Parameter muss eines der folgenden Elemente enthalten:

- Der Name des LDAP-Attributs, in dem der Profilwert gespeichert wird. Die Benutzer-ID wird zum Beispiel im uid-Attribut im Benutzerverzeichnis gespeichert.

  **Hinweis:** Um die Leistung zu verbessern, indizieren Sie LDAP-Attribute, die in Suchanfragen in der Benutzerkonsole verwendet werden.

- Ein bekanntes Attribut (siehe Seite 79). Wenn Sie ein bekanntes Attribut bereitstellen, berechnet CA IdentityMinder den Wert automatisch. Zum Beispiel bestimmt CA IdentityMinder nach dem Angeben des bekannten Attributs %ORG_MEMBERSHIP% basierend auf dem DN einer Eingabe jene Organisation, zu der die Eingabe gehört.

**Beschreibung**

Enthält die Beschreibung des Attributs

**displayName**

Gibt einen eindeutigen Namen für das Attribut an.

In der Benutzerkonsole wird der Anzeigename in der Liste der verfügbaren Attribute angezeigt, die einem Aufgabenfenster hinzugefügt werden können. Dieser Parameter ist erforderlich.

**Hinweis:** Sie dürfen den Anzeigenamen eines Attributs in der Verzeichniskonfigurationsdatei (directory.xml) nicht ändern. Um den Namen des Attributs in einem Aufgabenfenster zu ändern, geben Sie in der Aufgabenfensterdefinition eine Bezeichnung für das Attribut an. Weitere Informationen finden Sie im *Administrationshandbuch*.

**valuetype**

Gibt den Datentyp des Attributs an. Die folgenden Werte sind gültig:

**Zeichenfolge**

Der Wert kann eine beliebige Zeichenfolge sein.

Dies ist der Standardwert.

**Integer**

Der Wert muss eine Ganzzahl sein.

**Hinweis:** Der Parameter "Integer" unterstützt keine Dezimalzahlen.

**Number**

Der Wert muss eine Ganzzahl sein. Der Parameter "Number" unterstützt Dezimalzahlen.

**Datum**

Der Wert muss sich in ein gültiges Datum nach folgendem Muster auflösen lassen:

MM/TT/JJJJ

**ISODate**

Der Wert muss sich in ein gültiges Datum nach dem Muster JJJJ-MM-TT auflösen lassen.

**UnicenterDate**

Der Wert muss sich in ein gültiges Datum nach dem Muster JJJJJJJTTT auflösen lassen. Dabei gilt:

"JJJJJJJ" ist eine siebenstellige Darstellung für ein Jahr, bei dem am Anfang vor der eigentlichen Jahreszahl drei Nullen stehen. Beispiel: 0002008

"TTT" ist eine dreistellige Darstellung für einen Tag, bei dem am Anfang je nach Bedarf Nullen gesetzt werden. Die gültigen Werte umfassen hierbei den Bereich von 001 bis 366.

**Strukturiert**

Dieser Typ von Attribut besteht aus strukturierten Daten, die es einem einzelnen Attributwert ermöglichen, mehrere verknüpfte Werte zu speichern. Zum Beispiel enthält ein strukturiertes Attribut etwa Werte zu Vornamen, Nachnamen oder E-Mail-Adressen.

Bestimmte Endpunkttypen verwenden diese Attribute, werden aber durch CA IdentityMinder verwaltet.

**Hinweis:** CA IdentityMinder kann strukturierte Attribute in einer Tabelle in der Benutzerkonsole anzeigen. Wenn Benutzer Werte in der Tabelle bearbeiten, werden die Werte im Benutzerspeicher gespeichert und zurück zum Endpunkt übertragen. Weitere Informationen zum Anzeigen von Attributen mit mehreren Werten finden Sie im *Administrationshandbuch*.

**required**

Zeigt folgendermaßen an, ob das Attribut erforderlich ist:

- True - Das Attribut ist erforderlich.
- False - Das Attribut ist optional (Standard).

**Hinweis:** Wenn ein Attribut für einen LDAP-Verzeichnisserver erforderlich ist, legen Sie den erforderlichen Parameter auf "Wahr" (True) fest.

**mehrwertig**

Zeigt an, ob das Attribut mehrere Werte aufweisen kann. So ist zum Beispiel das Attribut der Gruppenmitgliedschaft mehrwertig, damit das Benutzer-DN jedes Gruppenmitglieds gespeichert werden kann. Die folgenden Werte sind gültig:

- True - Das Attribut kann mehrere Werte aufweisen.
- False - Das Attribut kann nur einen Einzelwert (Standard) aufweisen.

**Wichtig!** Die Attribute der Gruppenmitgliedschaft und der Admin-Rollen müssen in der Benutzerobjekt-Definition mehrwertig sein.

**wellknown**

Definiert den Namen des bekannten Attributs.

Bekannte Attribute haben eine bestimmte Bedeutung in CA IdentityMinder (siehe Seite 79). Sie werden über die Syntax identifiziert:

%ATTRIBUTENAME%

**maxlength**

Definiert die maximale Länge, die der Wert eines Attributs haben kann. Legen Sie den maxlength-Parameter auf 0 fest, um eine unbegrenzte Länge anzugeben.

**Hinweis:** Dieser Parameter ist erforderlich.

**permission**

Zeigt an, ob der Wert eines Attributs in einem Aufgabenfenster geändert werden kann. Die folgenden Werte sind gültig:

**READONLY**

Der Wert wird angezeigt, kann aber nicht geändert werden.

**WRITEONCE**

Der Wert kann nicht mehr geändert werden, nachdem das Objekt erstellt wurde. Zum Beispiel kann eine Benutzer-ID nicht geändert werden, nachdem der Benutzer erstellt wurde.

**READWRITE**

Der Wert kann geändert werden (Standardeinstellung).

**hidden**

Zeigt an, ob ein Attribut in CA IdentityMinder-Aufgabenformularen angezeigt wird. Die folgenden Werte sind gültig:

- True - Das Attribut wird den Benutzern nicht angezeigt.
- False - Das Attribut wird den Benutzern angezeigt (Standardeinstellung).

Logische Attribute verwenden verborgene Attribute.

**Hinweis:** Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

**system**

Gibt ausschließlich die von CA IdentityMinder verwendeten Attribute an. Benutzer in der Benutzerkonsole sollen die Attribute nicht ändern. Die folgenden Werte sind gültig:

- True - Benutzer dürfen das Attribut nicht ändern. Das Attribut wird auf der CA IdentityMinder-Benutzeroberfläche ausgeblendet.
- Falsch - Benutzer können dieses Attribut ändern. Das Attribut ist verfügbar, um zu Aufgabenfenstern auf der CA IdentityMinder-Benutzeroberfläche hinzugefügt zu werden. (Standard)

**validationruleset**

Verknüpft einen Validierungsregelsatz mit dem Attribut.

Überprüfen Sie, dass der Validierungsregelsatz, den Sie angeben, in einem ValidationRuleSet-Element in der Verzeichniskonfigurationsdatei definiert ist.

**objectclass**

Zeigt die LDAP-Hilfsklasse für ein Benutzer-, Gruppen- oder Organisationsattribut an, wenn das Attribut nicht Teil der im ImsManagedObject-Element angegebenen primären Objektklasse ist.

Nehmen Sie zum Beispiel an, dass die primäre Objektklasse für Benutzer "top", "person" und "organizationalperson" ist, wodurch die folgenden Benutzerattribute definiert werden:

- allgemeiner Name (cn)
- Zuname (sn)
- Benutzer-ID (uid)
- Kennwort (userPassword)

Um das Attribut "employeeID" einzuschließen, das in der Mitarbeiter-Hilfsklasse definiert wird, fügen Sie die folgende Attributbeschreibung hinzu:

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

## Geben Sie Attributbeschreibungen an.

Das Beschreiben von Attributen beinhaltet die folgenden Schritte:

1. Lesen Sie die zugehörigen Abschnitte zu den folgenden Themen:
   - CA Directory - Überlegungen (siehe Seite 77)
   - Microsoft Active Directory-Überlegungen (siehe Seite 78)
   - IBM-Verzeichnisserver-Überlegungen (siehe Seite 78)
   - Oracle Internet Directory-Überlegungen (siehe Seite 79)
2. Führen Sie in den Benutzerobjekt-, Gruppenobjekt- und Organisationsobjekt-Abschnitten der Verzeichniskonfigurationsdatei die folgenden Aktionen durch:
   - Ändern Sie die Standardattributbeschreibungen, um Ihre Verzeichnisattribute zu beschreiben.
   - Erstellen Sie neue Attributbeschreibungen, indem Sie eine vorhandene Beschreibung kopieren und Werte nach Bedarf ändern.

   **Hinweis:** Nehmen Sie an, dass eine neue Attributbeschreibung erstellt und ein physisches Attribut angegeben wird. Stellen Sie sicher, dass das physische Attribut in der Objektklasse (oder Klassen) vorhanden ist, die Sie für den Objekttyp angegeben haben.

3. (Optional) Ändern Sie die Anzeigeeinstellungen (siehe Seite 74) für das Attribut, um ein Anzeigen sensibler Information, wie etwa Kennwörter oder Gehälter, in der Benutzerkonsole zu verhindern.
4. (Optional) Konfigurieren Sie eine Standardsortierreihenfolge.
5. Wenn Sie ein Verzeichnis mit einer flachen Struktur oder einer flachen Benutzerstruktur oder ein Verzeichnis, das Organisationen ausschließt, verwalten, navigieren Sie zum Abschnitt "Beschreiben der Benutzerverzeichnisstruktur (siehe Seite 87)".

## Verwalten vertraulicher Attribute

CA IdentityMinder bietet die folgenden Methoden für die Verwaltung vertraulicher Attribute:

- Datenklassifizierungen für Attribute

  Mithilfe von Datenklassifizierungen können Sie Anzeige- und Verschlüsselungseigenschaften für Attribute in der Verzeichniskonfigurationsdatei (directory.xml) festlegen.

  Sie können Datenklassifizierungen, die vertrauliche Attribute verwalten, wie folgt definieren:

  - Zeigen Sie in den CA IdentityMinder-Aufgabenfenstern den Wert eines Attributs als Reihe von Sternchen an.

    Zum Beispiel können Sie Kennwörter als Sternchen anstelle von Klartext anzeigen.

  - Blenden Sie den Attributwert in den Fenstern "Gesendete Aufgaben anzeigen" aus.

    Mithilfe dieser Option können Sie Attribute ausblenden, damit Administratoren sie nicht sehen. Zum Beispiel können Gehaltsdetails wie die Höhe des Gehalts vor Administratoren verborgen werden, die den Aufgabenstatus in CA IdentityMinder anzeigen, aber keine Gehaltsdetails anzeigen müssen.

  - Ignorieren Sie bestimmte Attribute, wenn Sie eine Kopie eines vorhandenen Objekts erstellen.
  - Verschlüsseln von Attributen

- Feldtypen in Aufgabenprofilfenstern

  Wenn Sie ein Attribut nicht in der directory.xml-Datei ändern möchten, legen Sie die Anzeigeeigenschaft für das Attribut in den Bildschirmdefinitionen fest, in denen das vertrauliche Attribut angezeigt wird.

  Mithilfe des Feldtyps können Sie Attribute wie Kennwörter als Reihe von Sternchen anstelle von Klartext anzeigen.

  **Hinweis**: Weitere Informationen zum Feldtyp für vertrauliche Attribute finden Sie in den Abschnitten zu Feldtypen in der Benutzerkonsolen-Hilfe.

## Datenklassifizierungs-Attribute

Das Datenklassifizierungs-Element bietet eine Methode für das Zuordnen von zusätzlichen Eigenschaften zu einer Attributbeschreibung. Die Werte in diesem Element legen fest, wie CA IdentityMinder das Attribut verarbeitet. Dieses Element unterstützt die folgenden Parameter:

- sensitive

  Hat zur Folge, dass CA IdentityMinder das Attribut als Reihe von Sternchen (*) in den Fenstern "Gesendete Aufgaben anzeigen" anzeigt. Dieser Parameter verhindert, dass alte und neue Werte für das Attribut in den Fenstern "Gesendete Aufgaben anzeigen" als Klartext angezeigt werden.

  Wenn Sie eine Kopie eines vorhandenen Benutzers in der Benutzerkonsole erstellen, verhindert dieser Parameter außerdem, dass das Attribut zum neuen Benutzer kopiert wird.

- vst_hide

  Blendet das Attribut im Fenster "Ereignisdetails" auf der Registerkarte "Gesendete Aufgaben anzeigen" aus. Im Gegensatz zu vertraulichen Attributen, die als Sternchen angezeigt werden, werden vst_hidden-Attribute nicht angezeigt.

  Sie können diesen Parameter verwenden, damit Änderungen an einem Attribut, beispielsweise dem Gehalt, nicht im Fenster "Gesendete Aufgaben anzeigen" angezeigt werden.

- ignore_on_copy

  Hat zur Folge, dass CA IdentityMinder ein Attribut ignoriert, wenn ein Administrator eine Kopie eines Objekts in der Benutzerkonsole erstellt. Nehmen Sie zum Beispiel an, dass Sie ignore_on_copy für das Kennwortattribut eines Benutzerobjekts angegeben haben. Wenn Sie ein Benutzerprofil kopieren, überträgt CA IdentityMinder das Kennwort des aktuellen Benutzers nicht auf das neue Benutzerprofil.

- AttributeLevelEncrypt

  Verschlüsselt Attributwerte, wenn sie im Benutzerspeicher gespeichert werden. Wenn CA IdentityMinder für FIPS 140-2 aktiviert ist, verwendet CA IdentityMinder die RC2-Verschlüsselung oder die FIPS 140-2-Verschlüsselung.

  Weitere Informationen zur Unterstützung von FIPS 140-2 in CA IdentityMinder finden Sie im *Konfigurationshandbuch*.

  Die Attribute werden während Laufzeit als Klartext angezeigt.

  **Hinweis:** Um zu verhindern, dass Attribute in Fenstern als Klartext angezeigt werden, können Sie ein Element zu verschlüsselten Attributen hinzufügen, das sie als vertrauliche Daten klassifiziert. Weitere Informationen finden Sie unter Hinzufügen von Verschlüsselung auf Attributebene (siehe Seite 75).

- PreviouslyEncrypted

  Hat zur Folge, dass CA IdentityMinder alle verschlüsselte Werte im Attribut erkennt und entschlüsselt, wenn das Objekt im Benutzerspeicher aufgerufen wird.

  Mithilfe dieser Datenklassifizierung können Sie alle zuvor verschlüsselten Werte entschlüsseln.

  Der Klartextwert wird im Speicher gespeichert, wenn Sie das Objekt speichern.

## Konfigurieren von Datenklassifizierungs-Attributen

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei nach dem Attribut.
2. Fügen Sie das folgende Attribut nach der Attributbeschreibung hinzu:

   <DataClassification name="*parameter*">

   **parameter**

   Stellt einen der folgenden Parameter dar:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Eine Attributbeschreibung, die das Datenklassifizierungs-Attribut "vst_hide" enthält, entspricht zum Beispiel in etwa dem folgenden Code:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

## Verschlüsselung auf Attributebene

Sie können ein Attribut im Benutzerspeicher verschlüsseln, indem Sie eine AttributeLevelEncypt-Datenklassifizierung für dieses Attribut in der Verzeichniskonfigurationsdatei (directory.xml) angeben. Wenn die Verschlüsselung auf Attributebene aktiviert ist, verschlüsselt CA IdentityMinder den Wert dieses Attributs, bevor es im Benutzerspeicher gespeichert wird. Das Attribut wird in der Benutzerkonsole als Klartext angezeigt.

**Hinweis:** Um zu verhindern, dass Attribute in Fenstern als Klartext angezeigt werden, können Sie ein Element zu verschlüsselten Attributen hinzufügen, das sie als vertrauliche Daten klassifiziert. Weitere Informationen finden Sie unter Hinzufügen von Verschlüsselung auf Attributebene (siehe Seite 75).

Wenn die FIPS 140-2-Unterstützung aktiviert ist, wird das Attribut mithilfe der RC2-Verschlüsselung oder FIPS 140-2-Verschlüsselung verschlüsselt.

Beachten Sie Folgendes, bevor Sie die Verschlüsselung auf Attributebene implementieren:

- CA IdentityMinder kann bei einer Suche keine verschlüsselten Attribute finden.

  Nehmen Sie an, dass ein verschlüsseltes Attribut einer Mitglieds-, Admin- oder Eigentümerrichtlinie bzw. einer Identitätsrichtlinie hinzugefügt wird. CA IdentityMinder kann die Richtlinie nicht richtig auflösen, weil eine Suche nach dem Attribut nicht möglich ist.

  Ziehen Sie in Erwägung, das Attribut in der directory.xml-Datei auf searchable="false" festzulegen, zum Beispiel:

  ```
  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>
  ```

- Wenn CA IdentityMinder einen gemeinsamen Benutzerspeicher und ein gemeinsames Bereitstellungsverzeichnis verwendet, verschlüsseln Sie nicht die Bereitstellungsserver-Attribute.

- Aktivieren Sie AttributeLevelEncrypt nicht für Benutzerkennwörter in Umgebungen, die den folgenden Kriterien entsprechen:

  - Umfassen eine CA SiteMinder-Integration und
  - Speichern Benutzer in einer relationalen Datenbank

  Wenn CA IdentityMinder mit CA SiteMinder integriert wird, führen verschlüsselte Kennwörter zu Problemen, wenn neue Benutzer versuchen, sich anzumelden, und Kennwörter als Klartext eingeben.

- Wenn Sie die Verschlüsselung auf Attributebene für einen Benutzerspeicher aktivieren, der von anderen Anwendungen als CA IdentityMinder verwendet wird, können die anderen Anwendungen das verschlüsselte Attribut nicht verwenden.

## Hinzufügen von Verschlüsselung auf Attributebene

Nehmen Sie an, dass Sie eine Verschlüsselung auf Attributebene für ein CA IdentityMinder-Verzeichnis hinzugefügt haben. CA IdentityMinder verschlüsselt automatisch vorhandene Klartext-Attributwerte, wenn Sie das Objekt speichern, das dem Attribut zugeordnet ist. Wenn Sie zum Beispiel das Kennwortattribut verschlüsseln, wird beim Speichern des Benutzerprofils das Kennwort verschlüsselt.

**Hinweis**: Um den Attributwert zu verschlüsseln, muss die Aufgabe, die Sie zum Speichern des Objekts verwenden, das Attribut einschließen. Um das Kennwortattribut im vorherigen Beispiel zu verschlüsseln, vergewissern Sie sich, dass das Kennwortfeld der Aufgabe hinzugefügt wird, die Sie zum Speichern des Objekts verwenden, zum Beispiel die Aufgabe "Benutzer ändern".

Alle neuen Objekte werden mit verschlüsselten Werten im Benutzerspeicher erstellt.

**Gehen Sie wie folgt vor:**

1. Führen Sie eine der folgenden Aufgaben aus:
   - Erstellen Sie ein CA IdentityMinder-Verzeichnis.
   - Aktualisieren Sie ein vorhandenes Verzeichnis, indem Sie die Verzeichniseinstellungen exportieren.
2. Fügen Sie dem Attribut, das Sie in der directory.xml-Datei verschlüsseln möchten, die folgenden Datenklassifizierungs-Attribute hinzu:

   **AttributeLevelEncrypt**

   Behalten Sie den Attributwert im Benutzerspeicher in verschlüsselter Form bei.

   **sensitive (optional)**

   Blendet den Attributwert in CA IdentityMinder-Fenstern aus. Ein Kennwort wird zum Beispiel als Reihe von Sternchen (*) angezeigt.

   Beispiel:
   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0" searchable="false">
   <DataClassification name="AttributeLevelEncrypt"/>
   <DataClassification name="sensitive"/>
   ```
3. Wenn Sie ein CA IdentityMinder-Verzeichnis erstellt haben, ordnen Sie das Verzeichnis einer Umgebung zu.
4. Um zu erzwingen, dass CA IdentityMinder alle Werte sofort verschlüsselt, ändern Sie alle Objekte mithilfe des Massendatenladers.

   **Hinweis**: Weitere Informationen zum Massendatenlader finden Sie im *Administrationshandbuch*.

## Entfernen der Verschlüsselung auf Attributebene

Wenn im CA IdentityMinder-Verzeichnis ein verschlüsseltes Attribut enthalten ist, dessen Wert als Klartext gespeichert ist, können Sie die AttributeLevelEncrypt-Datenklassifizierung entfernen.

Nachdem die Datenklassifizierung entfernt worden ist, werden die neuen Attributwerte in CA IdentityMinder nicht mehr verschlüsselt. Vorhandene Werte werden entschlüsselt, wenn Sie das Objekt speichern, das dem Attribut zugeordnet wird.

**Hinweis**: Um den Attributwert zu entschlüsseln, muss die Aufgabe, die Sie zum Speichern des Objekts verwenden, das Attribut einschließen. Um zum Beispiel ein Kennwort für einen vorhandenen Benutzer zu entschlüsseln, speichern Sie das Benutzerobjekt mit einer Aufgabe, die das Kennwortfeld enthält, beispielsweise die Aufgabe "Benutzer ändern".

Um zu erzwingen, dass CA IdentityMinder alle verschlüsselten Werte erkennt und entschlüsselt, die für das Attribut im Benutzerspeicher verbleiben, können Sie eine andere Datenklassifizierung, PreviouslyEncrypted, angeben. Der Klartextwert wird im Benutzerspeicher gespeichert, wenn Sie das Objekt speichern.

**Hinweis**: Durch die Datenklassifizierung "PreviouslyEncrypted" wird bei jedem Laden des Objekts der Verarbeitungsaufwand erhöht. Um Leistungsbeeinträchtigungen zu verhindern, können Sie die Datenklassifizierung "PreviouslyEncrypted" hinzufügen, jedes Objekt, dem dieses Attribut zugeordnet ist, laden und speichern und anschließend die Datenklassifizierung wieder entfernen. Mit dieser Methode werden alle gespeicherten verschlüsselten Werte automatisch in gespeicherten Klartext konvertiert.

**Gehen Sie wie folgt vor:**

1. Exportieren Sie die Verzeichniseinstellungen für das entsprechende CA IdentityMinder-Verzeichnis.
2. Entfernen Sie in der directory.xml-Datei die Datenklassifizierung "AttributeLevelEncrypt" für Attribute, die Sie entschlüsseln möchten.
3. Wenn Sie erzwingen möchten, dass CA IdentityMinder zuvor verschlüsselte Werte entfernt, fügen Sie das Datenklassifizierungs-Attribut "PreviouslyEncrypted" hinzu.

   Beispiel:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```
4. Um zu erzwingen, dass CA IdentityMinder alle Werte sofort entschlüsselt, ändern Sie alle Objekte mithilfe des Massendatenladers.

   **Hinweis**: Weitere Informationen zum Massendatenlader finden Sie im *Administrationshandbuch*.

## CA Directory - Überlegungen

Wenn Sie Attribute für einen CA Directory-Benutzerspeicher beschreiben, müssen Sie die folgenden Punkte beachten:

- Bei Attributnamen wird die Groß-/Kleinschreibung berücksichtigt.
- Die Verwendung des "seeAlso"-Attributs als das Attribut, welches eine selbstabonnierende Gruppe angibt, kann zu Fehlern führen, wenn Administratoren Gruppen erstellen.

Die Verwendung des Foto-Attributs als das Attribut, welches den Status eines Benutzerkontos (aktiviert oder deaktiviert) angibt, kann zu Fehlern führen, wenn ein Administrator einen Benutzer erstellt.

**Hinweis:** Zusatzinformationen über CA-Directory-Anforderungen können Sie der CA-Directory-Dokumentation entnehmen.

## Microsoft Active Directory-Überlegungen

Wenn Sie Attribute für Active Directory beschreiben, beachten Sie die folgenden Punkte:

- Der Fall der in den Attributbeschreibungen spezifizierten Attribute muss mit dem Fall der Attribute unter Active Directory übereinstimmen. Wenn Sie zum Beispiel das unicodePwd-Attribut als das Attribut zum Speichern von Benutzerkennwörtern auswählen, geben Sie "unicodePwd" (mit großem P) in der Verzeichniskonfigurationsdatei an.
- Vergewissern Sie sich bei Benutzer- und Gruppenobjekten, dass Sie das sAMAccountName-Attribut einschließen.

## IBM-Verzeichnisserver-Überlegungen

Wenn Sie Attribute für ein Benutzerverzeichnis des IBM-Verzeichnisservers beschreiben, müssen Sie die folgenden Abschnitte ansehen:

- Gruppen in Verzeichnisserver-Verzeichnissen (siehe Seite 78)
- Die Objektklasse "Top" in der Organisationsobjekt-Beschreibung (siehe Seite 79)

### Gruppen in Verzeichnisserver-Verzeichnissen

Der IBM-Verzeichnisserver verlangt, dass Gruppen mindestens ein Mitglied enthalten. Um dieser Anforderung zu entsprechen, fügt CA IdentityMinder einen *Dummy-Benutzer* als Mitglied einer neuen Gruppe hinzu, wenn die Gruppe erstellt wird.

### Konfigurieren Sie einen Dummy-Benutzer.

**Gehen Sie wie folgt vor:**

1. Machen Sie im Abschnitt "Gruppenobjekt" der Verzeichniskonfigurationsdatei die folgenden Elemente ausfindig:

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   **Hinweis:** Wenn diese Elemente in der Verzeichniskonfigurationsdatei nicht vorhanden sind, fügen Sie sie genau so hinzu, wie sie hier angezeigt werden.

2. Ersetzen Sie ##DUMMY_USER_DN durch ein Benutzer-DN. CA IdentityMinder fügt dieses DN als Mitglied aller neuen Gruppen hinzu.

   **Hinweis:** Wenn Sie das DN eines vorhandenen Benutzers angeben, wird dieser Benutzer als Mitglied aller Gruppen von CA IdentityMinder angezeigt. Um zu verhindern, dass der *Dummy-Benutzer* als ein Gruppenmitglied angezeigt wird, geben Sie ein DN an, das nicht im Verzeichnis vorhanden ist.

3. Speichern Sie die Verzeichniskonfigurationsdatei.

### Die Objektklasse "Top" in der Organisationsobjekt-Beschreibung

**Wichtig!** Schließen Sie in der Beschreibung des Organisationsobjekts in der Verzeichniskonfigurationsdatei die Objektklasse "Top" nicht ein.

Wenn zum Beispiel die Objektklasse des Organisationsobjekts "Top", "organizationalUnit", lautet, geben Sie die Objektklasse folgendermaßen an:

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

Das Einbinden von "Top" kann zu unvorhergesehenen Suchergebnissen führen.

### Oracle Internet Directory-Überlegungen

Wenn Sie Attribute für den Benutzerspeicher eines Oracle Internet Directory (OID) beschreiben, geben Sie LDAP-Attribute ausschließlich mithilfe kleingeschriebener Buchstaben an.

## Bekannte Attribute für einen LDAP-Benutzerspeicher

Bekannte Attribute haben eine bestimmte Bedeutung in CA IdentityMinder. Sie werden wie in der folgenden Syntax angezeigt identifiziert:

%*ATTRIBUTENAME*%

In dieser Syntax muss *ATTRIBUTENAME* großgeschrieben werden.

Ein bekanntes Attribut wird einem physischem Attribut mithilfe einer Attributbeschreibung (siehe Seite 123) zugeordnet.

In der folgenden Attributbeschreibung wird das Benutzerkennwort des Attributs dem bekannten Attribut %PASSWORD% zugeordnet, sodass CA IdentityMinder den Wert unter "userpassword" wie folgt als Kennwort betrachtet:

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Bestimmte bekannte Attribute sind erforderlich, andere sind optional.

## Bekannte Attribute für Benutzer

Eine Liste Benutzern bekannter Attribute und die Elemente, denen sie zugeordnet werden, ist im Folgenden ersichtlich:

**%ADMIN_ROLE_CONSTRAINT%**

Führt Zuordnungen zur Liste von Admin-Rollen eines Administrators durch.

Das physische Attribut, das zu %ADMIN_ROLE_CONSTRAINT% zuordnet, muss mehrwertig sein, um mehrere Rollen aufzunehmen.

Es wird empfohlen, das LDAP-Attribut zu indizieren, welches zu %ADMIN_ROLE_CONSTRAINT% zugeordnet wird.

**%CERTIFICATION_STATUS%**

Führt Zuordnungen zum Zertifizierungsstatus eines Benutzers durch.

Dieses Attribut ist erforderlich, um die Funktion der Benutzerzertifizierung zu verwenden.

**Hinweis**: Weitere Informationen zur Benutzerzertifizierung finden Sie im *Administrationshandbuch*.

**%DELEGATORS%**

Wird einer Liste mit Benutzern zugeordnet, die Arbeitselemente an den aktuellen Benutzer delegiert haben.

Dieses Attribut ist für die Verwendung der Delegierung erforderlich. Das physische Attribut, das %DELEGATORS% zugeordnet ist, muss mehrere Werte umfassen, und es muss Zeichenfolgen enthalten können.

**Wichtig!** Eine direkte Bearbeitung dieses Felds mit CA IdentityMinder-Aufgaben oder einem externen Tool hat beträchtliche Auswirkungen auf die Sicherheit.

**%EMAIL%**

Führt Zuordnungen zur E-Mail-Adresse eines Benutzers durch.

Macht es erforderlich, die Funktion der E-Mail-Benachrichtigung zu verwenden.

**%ENABLED_STATE%**

(Erforderlich)

Führt Zuordnungen zum Status eines Benutzers durch.

**Hinweis:** Dieses Attribut muss mit dem Attribut des Benutzerverzeichnisses mit deaktiviertem Kennzeichen in der SiteMinder-Benutzerverzeichnisverbindung übereinstimmen.

**%FIRST_NAME%**

Führt Zuordnungen zum Vornamen eines Benutzers durch.

**%FULL_NAME%**

Führt Zuordnungen zum Vor- und zum Nachnamen eines Benutzers durch.

**%IDENTITY_POLICY%**

Gibt die Liste von Identitätsrichtlinien an, die auf ein Benutzerkonto angewendet werden, sowie eine Liste von eindeutigen Policy-Xpress-Richtlinien-IDs, die für das Benutzerobjekt Aktionen zum Hinzufügen oder zum Entfernen durchgeführt haben.

CA IdentityMinder verwendet dieses Attribut, um festzulegen, ob die Anwendung einer Identitätsrichtlinie auf einen Benutzer erforderlich ist oder nicht. Es sei davon auszugehen, dass für die Richtlinie die Einstellung der einmaligen Anwendung aktiviert ist und dass die Richtlinie im Attribut %IDENTITY_POLICY% aufgelistet ist. CA IdentityMinder wendet die Änderungen in der Richtlinie nicht auf den Benutzer an.

**Hinweis**: Weitere Informationen zu Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

**%LAST_CERTIFIED_DATE%**

Führt Zuordnungen zu dem Datum durch, an dem die Rollen für einen Benutzer zertifiziert werden.

Die Verwendung der Benutzerzertifizierungsfunktion ist erforderlich.

**Hinweis**: Weitere Informationen zur Benutzerzertifizierung finden Sie im *Administrationshandbuch*.

**%LAST_NAME%**

Führt Zuordnungen zum Nachnamen eines Benutzers durch.

**%MEMBER_OF%**

Führt Zuordnungen zur Liste der Gruppen durch, bei denen der Benutzer ein Mitglied ist.

Das physische Attribut, das zu %MEMBER_OF% zuordnet, muss mehrwertig sein, um mehrere Gruppen aufzunehmen.

Die Verwendung dieses Attributs verbessert die Antwortzeit, wenn die Gruppen eines Benutzers gesucht werden.

Sie können dieses Attribut mit Active Directory oder einem Verzeichnisschema verwenden, das die Gruppenmitgliedschaft eines Benutzers im Benutzerobjekt verwaltet.

**%ORG_MEMBERSHIP%**

(Erforderlich)

Führt Zuordnungen zu dem DN jener Organisation durch, zu der der Benutzer gehört.

CA IdentityMinder verwendet dieses bekannte Attribut, um die Struktur eines Verzeichnisses (siehe Seite 87) zu bestimmen.

Dieses Attribut wird nicht benötigt, wenn das Benutzerverzeichnis keine Organisationen einschließt.

**%ORG_MEMBERSHIP_NAME%**

(Erforderlich)

Führt Zuordnungen zum benutzerfreundlichen Namen der Organisation durch, in der das Profil des Benutzers vorhanden ist.

Dieses Attribut wird nicht benötigt, wenn das Benutzerverzeichnis keine Organisationen einschließt.

**%PASSWORD%**

Führt Zuordnungen zum Kennwort eines Benutzers durch.

Dieses Attribut muss mit dem Kennwortattribut in der SiteMinder-Benutzerverzeichnisverbindung übereinstimmen.

**Hinweis:** Der Wert des Attributs %PASSWORD% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%PASSWORD_DATA%**

(Für die Unterstützung von Kennwortrichtlinien erforderlich.)

Gibt das Attribut an, das Kennwortrichtlinieninformationen verfolgt.

**Hinweis:** Der Wert des Attributs %PASSWORD_DATA% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%PASSWORD_HINT%**

(Erforderlich)

Führt Zuordnungen zu einem benutzerspezifischen Frage- und Antwortpaar durch. Das Frage- und Antwortpaar wird verwendet, wenn Benutzer ihre Kennwörter vergessen.

Um mehrere Frage- und Antwortpaare zu unterstützen, müssen Sie sicherstellen, dass das %PASSWORD_HINT%-Attribut mehrwertig ist.

Wenn Sie die Funktion der Kennwortdienste von SiteMinder verwenden, um Kennwörter zu verwalten, muss das Kennworthinweis-Attribut mit dem "Challenge/Response"-Attribut im SiteMinder-Benutzerverzeichnis übereinstimmen.

**Hinweis:** Der Wert des Attributs %PASSWORD% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%USER_ID%**

(Erforderlich)

Führt Zuordnungen zur ID eines Benutzers durch.

## Bekannte Attribute für Gruppen

Die folgenden Elemente stellen die Liste der Gruppe der bekannten Attribute dar:

**%GROUP_ADMIN_GROUP%**

Zeigt an, welches Attribut eine Liste von Gruppen speichert, die wiederum als Administratoren einer Gruppe fungieren können. Wenn zum Beispiel die Gruppe 1 ein Administrator der Gruppe A ist, wird Gruppe 1 im %GROUP_ADMIN_GROUP%-Attribut gespeichert.

**Hinweis:** Wenn Sie kein %GROUP_ADMIN_GROUP%-Attribut angeben, speichert CA IdentityMinder die Administratorgruppen im %GROUP_ADMIN%-Attribut.

**Hinweis:** Um eine Gruppe als Administrator einer anderen Gruppe hinzuzufügen, lesen Sie die entsprechenden Abschnitte im *Administrationshandbuch*.

**%GROUP_ADMIN%**

Zeigt an, welches Attribut die DNs der Administratoren einer Gruppe enthält.

Das physische Attribut, das zu %GROUP_ADMIN% zugeordnet ist, muss mehrwertig sein.

**%GROUP_DESC%**

Zeigt an, welches Attribut die Beschreibung einer Gruppe enthält.

**%GROUP_MEMBERSHIP%**

(Erforderlich)

Zeigt an, welches Attribut eine Liste der Mitglieder einer Gruppe enthält.

Das physische Attribut, das zu %GROUP_MEMBERSHIP% zugeordnet ist, muss mehrwertig sein.

Das bekannte %GROUP_MEMBERSHIP%-Attribut ist nicht für Provisioning-Benutzer-Verzeichnisse erforderlich.

**%GROUP_NAME%**

(Erforderlich)

Zeigt an, welches Attribut einen Gruppennamen speichert.

**%ORG_MEMBERSHIP%**

(Erforderlich)

Zeigt an, welches Attribut das DN der Organisation enthält, zu der die Gruppe gehört.

CA IdentityMinder verwendet dieses bekannte Attribut, um die Struktur des Verzeichnisses (siehe Seite 87) zu bestimmen.

Dieses Attribut wird nicht benötigt, wenn das Benutzerverzeichnis keine Organisationen einschließt.

**%ORG_MEMBERSHIP_NAME%**

Zeigt an, welches Attribut den benutzerfreundlichen Namen der Organisation enthält, in der die Gruppe vorhanden ist.

Dieses Attribut ist nicht für Benutzerverzeichnisse gültig, die keine Organisationen einschließen.

**%SELF_SUBSCRIBING%**

Zeigt an, welches Attribut entscheidet, ob Benutzer sich einer Gruppe (siehe Seite 86) anschließen können.

**%NESTED_GROUP_MEMBERSHIP%**

Zeigt an, welches Attribut eine Liste von Gruppen speichert, die wiederum als Mitglieder einer Gruppe fungieren können. Wenn zum Beispiel die Gruppe 1 ein Mitglied der Gruppe A ist, wird Gruppe 1 im %NESTED_GROUP_MEMBERSHIP%-Attribut gespeichert.

Wenn Sie kein %NESTED_GROUP_MEMBERSHIP%-Attribut angeben, speichert CA IdentityMinder verschachtelte Gruppen im %GROUP_MEMBERSHIP%-Attribut.

Um Gruppen als Mitglieder anderer Gruppen einzubinden, konfigurieren Sie den Support für verschachtelte Gruppen, wie in den Anweisungen zum Konfigurieren von dynamischen und verschachtelten Gruppen beschrieben.

**%DYNAMIC_GROUP_MEMBERSHIP%**

Zeigt an, welches Attribut die LDAP-Abfrage speichert, die eine dynamische Gruppe (siehe Seite 149) generiert.

**Hinweis:** Um die verfügbaren Attribute für das Gruppenobjekt zu erweitern, damit die %NESTED_GROUP_MEMBERSHIP%- und %DYNAMIC_GROUP_MEMBERSHIP%-Attribute eingebunden werden können, können Sie Hilfsobjektklassen verwenden.

## Bekannte Attribute zur Organisation

Die folgenden bekannten Attribute gelten ausschließlich für Umgebungen, die Organisationen unterstützen:

**%ORG_DESCR%**

Zeigt an, welches Attribut die Beschreibung einer Organisation enthält.

**%ORG_MEMBERSHIP%**

(Erforderlich)

Zeigt an, welches Attribut das DN der übergeordneten Organisation einer Organisation enthält.

**%ORG_MEMBERSHIP_NAME%**

Gibt an, welches Attribut den benutzerfreundlichen Namen der übergeordneten Organisation einer Organisation enthält.

**%ORG_NAME%**

(Erforderlich)

Gibt an, welches Attribut den Namen der Organisation enthält.

# Attribut %ADMIN_ROLE_CONSTRAINT%

Wenn Sie eine Admin-Rolle erstellen, geben Sie eine oder mehrere Regeln für die Rollenmitgliedschaft an. Die Rolle wird dann allen Benutzern erteilt, die die Mitgliedschaftsregeln erfüllen. Wenn zum Beispiel die Mitgliedschaftsregel für die Rolle "User Manager" "title=User Manager" lautet, wird Benutzern mit dem Titel "User Manager" die Rolle "User Manager" erteilt.

**Hinweis**: Weitere Informationen zu Regeln finden Sie im *Administrationshandbuch*.

%ADMIN_ROLE_CONSTRAINT% ermöglicht es Ihnen, ein Profilattribut anzugeben, in dem die Admin-Rollen eines Administrators gespeichert werden.

## So verwenden Sie das Attribut %ADMIN_ROLE_CONSTRAINT%

Um %ADMIN_ROLE_CONSTRAINT% als Einschränkung für alle Admin-Rollen zu verwenden, führen Sie die folgenden Aufgaben aus:

- Ordnen Sie das bekannte Attribut %ADMIN_ROLE_CONSTRAINT% einem mehrwertigen Profilattribut zu, um mehrere Rollen zu berücksichtigen.
- Wenn Sie eine Admin-Rolle in der Benutzerkonsole konfigurieren, vergewissern Sie sich über die folgende Einschränkung:

  `Die Admin-Rollen stimmen mit dem` *`Rollennamen`* `überein.`

  **role name**

  Definiert den Namen der Rolle, für die Sie die Einschränkung angeben, wie im folgenden Beispiel gezeigt:

  `"Admin-Rollen" stimmt mit "User Manager" überein.`

**Hinweis:** "Admin-Rollen" ist der Standardanzeigename für das Attribut %ADMIN_ROLE_CONSTRAINT%.

# Konfigurieren von bekannten Attributen

Führen Sie zum Konfigurieren bekannter Attribute die folgenden Schritte aus.

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei nach dem folgenden Zeichen:

   ##

2. Ersetzen Sie den mit ## beginnenden Wert durch das entsprechende LDAP-Attribut.
3. Wiederholen Sie die Schritte 1 und 2, bis Sie alle erforderlichen Werte ersetzt haben.

4. Ordnen Sie optional die bekannten Attribute physischen Attributen zu, sofern erforderlich.
5. Speichern Sie die Verzeichniskonfigurationsdatei.

# Beschreiben der Benutzerverzeichnisstruktur

CA IdentityMinder verwendet das bekannte Attribut %ORG_MEMBERSHIP%, um die Struktur eines Benutzerverzeichnisses zu bestimmen.

Das Verfahren zum Beschreiben der Benutzerverzeichnisstruktur hängt vom Typ der Verzeichnisstruktur ab.

## So beschreiben Sie eine hierarchische Verzeichnisstruktur

Die Verzeichniskonfigurationsdatei für eine hierarchische Verzeichnisstruktur ist bereits konfiguriert. Dadurch müssen Sie die Beschreibung des Attributs %ORG_MEMBERSHIP% nicht ändern.

## So beschreiben Sie eine flache Benutzerverzeichnisstruktur

**Gehen Sie wie folgt vor:**

1. Suchen Sie die Beschreibung des Attributs %ORG_MEMBERSHIP% im Abschnitt für Benutzerobjekte der Datei "directory.xml".
2. Ersetzen Sie im Parameter "physicalname" das Attribut %ORG_MEMBERSHIP% durch den Namen des Attributs, in dem die Organisation des Benutzers gespeichert ist.

## So beschreiben Sie eine flache Verzeichnisstruktur

**Gehen Sie wie folgt vor:**

1. Suchen Sie die Beschreibung des Attributs %ORG_MEMBERSHIP% im Abschnitt für Benutzerobjekte der Datei "directory.xml".
2. Ersetzen Sie im Parameter "physicalname" das Attribut %ORG_MEMBERSHIP% durch den Namen des Attributs, in dem die Organisation des Benutzers gespeichert ist.
3. Wiederholen Sie Schritt 1 im Abschnitt für Gruppenobjekte.
4. Ersetzen Sie im Parameter "physicalname" das Attribut %ORG_MEMBERSHIP% durch den Namen des Attributs, in dem die Organisation der Gruppe gespeichert ist.

## So beschreiben Sie ein Benutzerverzeichnis, das keine Organisationen unterstützt

Vergewissern Sie sich, dass keine Objektbeschreibungen oder bekannten Attribute für Organisationen in der Datei "directory.xml" definiert sind.

# So konfigurieren Sie Gruppen

Für die Konfiguration lassen sich Gruppen folgendermaßen aufteilen:

- Selbstabonnierende Gruppen
- Dynamische und verschachtelte Gruppen

## Konfigurieren von selbstabonnierenden Gruppen

Um Self-Service-Benutzern den Beitritt zu Gruppen zu ermöglichen, können Sie in der Verzeichniskonfigurationsdatei die Unterstützung selbstabonnierender Gruppen konfigurieren.

Wenn sich ein Benutzer anmeldet, sucht CA IdentityMinder nach Gruppen in den angegebenen Organisationen und zeigt dem Benutzer die selbstabonnierenden Gruppen an.

**Gehen Sie wie folgt vor:**

1. Fügen Sie im Abschnitt für selbstabonnierende Gruppen das Element "SelfSubscribingGroups" wie folgt hinzu:

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. Fügen Sie Werte für die folgenden Parameter hinzu:

   **type**

   Gibt wie folgt an, wo CA IdentityMinder nach selbstabonnierenden Gruppen sucht:

   - NONE - CA IdentityMinder sucht nicht nach Gruppen. Geben Sie NONE an, wenn Sie verhindern möchten, dass Benutzer selbst Gruppen abonnieren.
   - ALL - CA IdentityMinder beginnt mit der Suche nach Gruppen im Stammverzeichnis. Geben Sie ALL an, wenn Benutzer im gesamten hierarchischen Verzeichnis Gruppen abonnieren können.

- INDICATEDORG - CA IdentityMinder sucht nach selbstabonnierenden Gruppen in der Organisation eines Benutzers und den zugehörigen Unterorganisationen. Wenn zum Beispiel das Profil eines Benutzers der Marketingorganisation angehört, sucht CA IdentityMinder nach selbstabonnierenden Gruppen in der Marketingorganisation und in allen Unterorganisationen.
- SPECIFICORG - CA IdentityMinder sucht in einer bestimmten Organisation. Geben Sie den definierten Namen (DN) der jeweiligen Organisation im Parameter "org" an.

**org**

Gibt die eindeutige Kennung der Organisation an, in der CA IdentityMinder nach selbstabonnierenden Gruppen sucht.

**Hinweis:** Stellen Sie sicher, dass Sie den Parameter "org" angeben, wenn "type=SPECIFICORG" festgelegt ist.

Nachdem Sie die Unterstützung für selbstabonnierende Gruppen im CA IdentityMinder-Verzeichnis konfiguriert haben, können CA IdentityMinder-Administratoren angeben, welche Gruppen in der Benutzerkonsole selbstabonnierend sind.

**Hinweis**: Weitere Informationen zur Verwaltung von Gruppen finden Sie im *Administrationshandbuch*.

## Konfigurieren von dynamischen und verschachtelten Gruppen

Wenn Sie einen LDAP-Benutzerspeicher verwalten, können Sie Unterstützung für die folgenden Typen von Gruppen in der Verzeichniskonfigurationsdatei konfigurieren:

**Dynamische Gruppen**

Ermöglicht Ihnen die Definition von Gruppenmitgliedschaften, indem Sie in der Benutzerkonsole eine LDAP-Filterabfrage dynamisch angeben. Bei Verwendung von dynamischen Gruppen müssen Administratoren nicht einzeln nach Gruppenmitgliedern suchen und diese hinzufügen.

**Verschachtelte Gruppen**

Ermöglicht es Ihnen, Gruppen als Mitglieder anderer Gruppen hinzuzufügen.

Sie können dynamische und verschachtelte Gruppen mithilfe der Verzeichniskonfigurationsdatei aktivieren.

**Gehen Sie wie folgt vor:**

1. Ordnen Sie nach Bedarf die folgenden bekannten Attribute (siehe Seite 83) physischen Attributen für das verwaltete Objekt "Gruppe" zu:

   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   **Hinweis**: Das ausgewählte physische Attribut muss mehrere Werte unterstützen.

2. Fügen Sie im Abschnitt für das Verzeichnisgruppenverhalten das folgende GroupTypes-Element hinzu:

   ```
   <GroupTypes type=group>
   ```

3. Geben Sie einen Wert für den folgenden Parameter ein:

   **group**

   Aktiviert die Unterstützung für dynamische und verschachtelte Gruppen. Die folgenden Werte sind gültig:

   - NONE - CA IdentityMinder unterstützt keine dynamischen und verschachtelten Gruppen.
   - ALL - CA IdentityMinder unterstützt dynamische und verschachtelte Gruppen.
   - DYNAMIC - CA IdentityMinder unterstützt nur dynamische Gruppen.
   - NESTED - CA IdentityMinder unterstützt nur verschachtelte Gruppen.

Nachdem Sie die Unterstützung für dynamische und verschachtelte Gruppen im CA IdentityMinder-Verzeichnis konfiguriert haben, können CA IdentityMinder-Administratoren angeben, welche Gruppen in der Benutzerkonsole dynamisch und welche verschachtelt sind.

**Hinweis:** Beachten Sie, dass Sie den Gruppentyp auf NESTED oder ALL festgelegt haben, *ohne* den bekannten Parameter %NESTED_GROUP_MEMBERSHIP% festzulegen. In diesem Fall speichert CA IdentityMinder sowohl die verschachtelten Gruppen als auch die Benutzer in dem bekannten Parameter %GROUP_MEMBERSHIP%. Die Verarbeitung von Gruppenmitgliedschaften kann geringfügig langsamer sein.

## Hinzufügen von Unterstützung für Gruppen als Gruppenadministrator

Bei Verwaltung eines LDAP-Benutzerspeichers können Sie festlegen, dass Gruppen als Administratoren anderer Gruppen fungieren können. Wenn Sie eine Gruppe als Administrator zuweisen, sind nur die Administratoren dieser Gruppe Administratoren der anderen angegebenen Gruppe. Die Mitglieder der angegebenen Administratorgruppe sind nicht berechtigt, die Gruppe zu verwalten.

**Gehen Sie wie folgt vor:**

1. Ordnen Sie das bekannte Attribut %GROUP_ADMIN_GROUP% einem physischen Attribut zu, in dem die Liste der Gruppen gespeichert ist, die als Administratoren dienen.

   **Hinweis**: Das ausgewählte physische Attribut muss mehrere Werte unterstützen.

   Unter Gruppieren bekannter Attribute (siehe Seite 83) finden Sie weitere Informationen über das Attribut %GROUP_ADMIN_GROUP%.

   **Hinweis**: Wenn Sie als Typ der Admin-Gruppe ALL festlegen, ohne das bekannte Attribut %GROUP_ADMIN_GROUP% festzulegen, speichert CA IdentityMinder die Administratorgruppen im Attribut %GROUP_ADMIN%.

2. Konfigurieren Sie im Abschnitt für das Verhalten von Verzeichnisadministratorgruppen das AdminGroupTypes-Element wie folgt:

   <AdminGroupTypes type="ALL">

   **Hinweis**: Die Standardeinstellung von "AdminGroupTypes" ist NONE.

Nachdem Sie die Unterstützung von Gruppen als Administratoren im CA IdentityMinder-Verzeichnis konfiguriert haben, können CA IdentityMinder-Administratoren in der Benutzerkonsole Gruppen als Administratoren von anderen Gruppen angeben.

# Validierungsregeln

Eine Validierungsregel setzt Anforderungen an Daten durch, die ein Benutzer in ein Feld des Aufgabenfensters eingibt. Die Anforderungen können festlegen, dass ein bestimmter Datentyp oder ein bestimmtes Format zu verwenden ist. Vergewissern Sie sich daher, ob die Daten im Kontext der anderen Daten im Aufgabenfenster gültig sind.

Validierungsregeln sind Profilattributen zugeordnet. CA IdentityMinder stellt sicher, dass die für ein Profilattribut eingegebenen Daten alle zugehörigen Validierungsregeln erfüllen, bevor eine Aufgabe verarbeitet wird.

Sie können Validierungsregeln definieren und sie Profilattributen in der Verzeichniskonfigurationsdatei zuordnen.

# Zusätzliche Eigenschaften des CA IdentityMinder-Verzeichnisses

Sie können die folgenden zusätzlichen Eigenschaften konfigurieren:

- Sortierreihenfolge der Suchergebnisse.
- Suche über mehrere Objektklassen, um zu überprüfen, dass ein neuer Benutzer nicht bereits vorhanden ist.
- Wartezeit, um zu verhindern, dass CA IdentityMinder vor Abschluss der Datenreplikation vom Master-LDAP-Verzeichnis zum Slave-LDAP-Verzeichnis das Zeitlimit überschreitet.

## Konfigurieren der Sortierreihenfolge

Sie können ein Sortierungsattribut für jedes verwaltete Objekt angeben, z. B. für Benutzer, Gruppen oder Organisationen. CA IdentityMinder verwendet dieses Attribut zum Sortieren der Suchergebnisse in benutzerdefinierter Business Logic, die Sie mit den CA IdentityMinder-APIs erstellen.

**Hinweis**: Das Sortierungsattribut wirkt sich nicht auf die Darstellung der Suchergebnisse in der Benutzerkonsole aus.

Wenn Sie zum Beispiel das cn-Attribut für das Benutzerobjekt angeben, sortiert CA IdentityMinder die Ergebnisse einer Suche nach Benutzern alphabetisch nach dem cn-Attribut.

**Gehen Sie wie folgt vor:**

1. Fügen Sie nach dem letzten IMSManagedObjectAttr-Element im Abschnitt für das verwaltete Objekt, auf das sich die Sortierreihenfolge bezieht, die folgenden Anweisungen hinzu:

   ```
   <PropertyDict name="SORT_ORDER">
       <Property name="ATTR">your_sort_attribute
       </Property>
   </PropertyDict>
   ```

2. Ersetzen Sie *your_sort_attribute* durch das Attribut, nach dem CA IdentityMinder die Suchergebnisse sortieren soll.

**Hinweis:** Geben Sie nur ein physisches Attribut an. Geben Sie kein bekanntes Attribut an.

Angenommen Sie möchten die Benutzer in den Suchergebnissen nach dem Wert des Attributs "cn" sortieren. Fügen Sie dazu nach dem letzten IMSManagedObjectAttr-Element im Abschnitt für Benutzerobjekte der Verzeichniskonfigurationsdatei die folgenden Elemente hinzu:

```
<!-- ******************** User Object ******************** -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

## Suchen über mehrere Objektklassen

Wenn Sie einen Benutzer erstellen, durchsucht CA IdentityMinder den Benutzerspeicher, um zu überprüfen, ob der Benutzer bereits vorhanden ist oder nicht. Diese Suche ist auf Benutzer beschränkt, für die eine Objektklasse in der Benutzerobjektdefinition in der Verzeichniskonfigurationsdatei (directory.xml) angegeben ist. Wird in diesen Objektklassen kein vorhandener Benutzer gefunden, versucht CA IdentityMinder, den Benutzer zu erstellen.

Ist ein Benutzer mit der gleichen eindeutigen Kennung (Benutzer-ID), aber einer anderen Objektklasse vorhanden, schlägt die Erstellung des Benutzers am LDAP-Server fehl. Am LDAP-Server wird daraufhin ein Fehler gemeldet, CA IdentityMinder erkennt diesen Fehler jedoch nicht. Es hat daher den Anschein, als würde CA IdentityMinder den Benutzer erfolgreich erstellen.

Um dieses Problem zu vermeiden, können Sie die Eigenschaft SEARCH_ACROSS_CLASSES konfigurieren, durch die CA IdentityMinder bei der Überprüfung auf vorhandene Benutzer diese über alle Objektklassendefinitionen hinweg sucht.

**Hinweis:** Diese Eigenschaft wirkt sich nur auf Suchen nach doppelten Benutzern aus, wenn Aufgaben wie das Erstellen eines Benutzers ausgeführt werden. Bei allen anderen Suchen gelten die Objektklasseneinschränkungen.

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei (directory.xml) das ImsManagedObject-Element, das das Benutzerobjekt beschreibt.
2. Fügen Sie das folgende PropertyDict-Element hinzu:

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

**Hinweis:** Das PropertyDict-Element muss das letzte Element im ImsManagedObject-Element sein, wie im folgenden Beispiel dargestellt:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

## Angeben der Wartezeit für Replikationen

In einer Bereitstellung, die eine Replikation zwischen Master- und Slave-LDAP-Verzeichnissen beinhaltet, können Sie den SiteMinder-Richtlinienserver so konfigurieren, dass er mit einem Slaveverzeichnis kommuniziert. Der Richtlinienserver erkennt in einer solchen Konfiguration automatisch Verweise auf das Masterverzeichnis, wenn Vorgänge ausgeführt werden, bei denen Daten in das LDAP-Verzeichnis geschrieben werden. Die Daten werden im Master-LDAP-Verzeichnis gespeichert und entsprechend dem Replikationsschema Ihrer Netzwerkressourcen im Slave-LDAP-Verzeichnis repliziert.

Wenn Sie in einer solchen Konfiguration ein Objekt in CA IdentityMinder erstellen, wird dieses im Masterverzeichnis erstellt und zusätzlich im Slaveverzeichnis repliziert. Während des Replikationsprozesses kann es zu Verzögerungen kommen, durch die der Erstellungsvorgang in CA IdentityMinder fehlschlägt.

Um dieses Problem zu vermeiden, können Sie in der Eigenschaft REPLICATION_WAIT_TIME die Wartezeit (in Sekunden) angeben, bevor CA IdentityMinder das Zeitlimit überschreitet.

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei (directory.xml) das ImsManagedObject-Element, das das Benutzerobjekt beschreibt.
2. Fügen Sie das folgende PropertyDict-Element hinzu:

```
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME"><time in seconds></Property>
</PropertyDict>
```

**Hinweis:** Das PropertyDict-Element muss das letzte Element im ImsManagedObject-Element sein, wie im folgenden Beispiel dargestellt:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME">800</Property>
</PropertyDict>
```

Wenn die keine Wartezeit für Replikationen definiert wird, wird der Standardwert 0 verwendet.

## Angeben von LDAP-Verbindungseinstellungen

Um die Leistung zu verbessern, können Sie die folgenden Parameter in der Verzeichniskonfigurationsdatei (directory.xml) angeben:

**Verbindungszeitlimit**

Gibt die maximale Zeit in Millisekunden an, die CA IdentityMinder ein Verzeichnis durchsucht, bevor die Suche beendet wird.

Diese Eigenschaft wird in der Verzeichniskonfigurationsdatei wie folgt angegeben:

com.sun.jndi.ldap.connect.timeout

**Connection Pool Max Size**

Gibt die maximale Anzahl von Verbindungen an, die CA IdentityMinder zum LDAP-Verzeichnis herstellen kann.

Diese Eigenschaft wird in der Verzeichniskonfigurationsdatei wie folgt angegeben:

com.sun.jndi.ldap.connect.pool.maxsize

**Connection Pool Default Size**

Gibt die Standardanzahl von Verbindungen zwischen CA IdentityMinder und dem LDAP-Verzeichnis an.

Diese Eigenschaft wird in der Verzeichniskonfigurationsdatei wie folgt angegeben:

com.sun.jndi.ldap.connect.pool.prefsize

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei (directory.xml) das ImsManagedObject-Element, das das Benutzerobjekt beschreibt.
2. Fügen Sie das folgende PropertyDict-Element hinzu:

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. Speichern Sie die Datei "directory.xml".

   CA IdentityMinder konfiguriert diese Einstellungen, wenn Sie das CA IdentityMinder-Verzeichnis mit dieser Datei erstellen.

# So verbessern Sie die Leistung von Verzeichnissuchen

Um die Leistung von Verzeichnissuchen nach Benutzern, Organisationen und Gruppen zu verbessern, führen Sie die folgenden Schritte aus:

- Indizieren Sie die Attribute, die Administratoren in Suchanfragen angeben können.

  **Hinweis:** In Oracle Internet Directory kann eine Suche fehlschlagen, wenn ein Attribut in einer Suchanfrage nicht indiziert ist.

- Konfigurieren Sie die Einstellungen für Seitengröße und maximale Zeilenanzahl (siehe Seite 97), um zu bestimmen, wie CA IdentityMinder große Suchen verarbeitet.
- Optimieren Sie das Benutzerverzeichnis. Weitere Informationen finden Sie in der Dokumentation zum verwendeten Benutzerverzeichnis.

## So verbessern Sie die Leistung von großen Suchen

Wenn CA IdentityMinder einen großen Benutzerspeicher verwaltet, reicht bei Suchen, die viele Ergebnisse zurückgeben, der Systemspeicher möglicherweise nicht aus. Um Speicherprobleme zu vermeiden, können Sie Beschräkungen für große Suchen definieren.

Die beiden folgenden Einstellungen bestimmen, wie CA IdentityMinder große Suchen verarbeitet:

- Maximale Zeilenanzahl

  Gibt die maximale Anzahl von Ergebnissen an, die CA IdentityMinder beim Durchsuchen eines Benutzerverzeichnisses zurückgeben kann. Wenn die Anzahl von Ergebnissen das Limit überschreitet, wird ein Fehler angezeigt.

- Seitengröße

  Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

  Beachten Sie beim Angeben der Seitengröße die folgenden Punkte:

  - Damit Sie die Option zur Festlegung der Seitengröße von Suchen verwenden können, muss der von CA IdentityMinder verwaltete Benutzerspeicher Paging unterstützen. Einige Benutzerspeichertypen erfordern jedoch zusätzliche Konfigurationsschritte, damit sie Paging unterstützen. Weitere Informationen finden Sie in den folgenden Themen:

    Konfigurieren von Paging-Unterstützung für Sun Java System Directory Server (siehe Seite 99)

    Konfigurieren von Paging-Unterstützung für Active Directory

  - Wenn der Benutzerspeicher kein Paging unterstützt und ein Wert für "maxrows" angegeben wird, verwendet CA IdentityMinder nur den Wert für "maxrows" zum Steuern der Suchgröße.

Sie können die maximale Zeilenanzahl und Seitengröße an den folgenden Positionen konfigurieren:

- Benutzerspeicher

  In den meisten Benutzerspeichern und Datenbanken können Sie Beschränkungen für die Suche konfigurieren.

  **Hinweis:** Weitere Informationen finden Sie in der Dokumentation zu dem verwendeten Benutzerspeicher oder zu der verwendeten Datenbank.

- CA IdentityMinder-Verzeichnis

  Sie können das DirectorySearch-Element (siehe Seite 58) in der verwendeten Verzeichniskonfigurationsdatei (directory.xml) konfigurieren, um das CA IdentityMinder-Verzeichnis zu erstellen.

  Standardmäßig ist der Wert für die maximale Zeilenanzahl und Seitengröße für vorhandene Verzeichnisse unbegrenzt. Für neue Verzeichnisse ist der Wert für die maximale Zeilenanzahl unbegrenzt und der Wert für die Seitengröße ist 2000.

- Definition für verwaltete Objekte

  Um die maximale Zeilenanzahl und Seitengröße für einen einzelnen Objekttyp anstatt für ein ganzes Verzeichnis festzulegen, konfigurieren Sie die *Definition für verwaltete Objekte* (siehe Seite 61) in der verwendeten Datei "directory.xml", um das CA IdentityMinder-Verzeichnis zu erstellen.

  Das Festlegen von Beschränkungen für einen verwalteten Objekttyp ermöglicht es Ihnen, Anpassungen basierend auf den Geschäftsanforderungen vorzunehmen. Zum Beispiel haben die meisten Unternehmen mehr Benutzer als Gruppen. Diese Unternehmen können nur Limits für Benutzerobjektsuchen festlegen.

- Aufgabensuchfenster

  Sie können die Anzahl der Suchergebnisse steuern, die Benutzern in den Such- und Listenfenstern der Benutzerkonsole angezeigt werden. Wenn die Ergebnisanzahl die maximale Anzahl von Ergebnissen pro Seite überschreitet, die für die Aufgabe definiert ist, werden den Benutzern Links zu weiteren Ergebnisseiten angezeigt.

  Diese Einstellung wirkt sich nicht auf die Anzahl der Ergebnisse aus, die von einer Suche zurückgegeben werden.

  **Hinweis:** Weitere Informationen zum Festlegen der Seitengröße in Such- und Listenfenstern finden Sie im *Administrationshandbuch*.

Wenn die maximale Zeilenanzahl und Seitengröße an mehreren Positionen definiert werden, gilt die jeweils spezifischste Einstellung. Zum Beispiel haben Einstellungen für verwaltete Objekte Vorrang vor Einstellungen auf Verzeichnisebene.

## Konfigurieren von Paging-Unterstützung für Sun Java System Directory Server

Sun Java System Directory Server unterstützt Virtual List View (VLV), eine Methode zum Zurückgeben von Suchergebnissen in einer bestimmten Reihenfolge oder in bestimmten Teilmengen. Diese Methode unterscheidet sich von der Simple Paged Results-Methode, von der CA IdentityMinder ausgeht.

Um VLV verwenden zu können, müssen Sie Berechtigungen festlegen und Indizes erstellen. CA IdentityMinder beinhaltet die folgenden Dateien, die Sie für die Paging-Unterstützung konfigurieren müssen:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Diese Dateien sind Teil des NeteAuto-Beispiels unter "samples\NeteAuto" in den Verwaltungstools.

Die Verwaltungstools werden in den folgenden Standardordnern installiert:

Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

**Gehen Sie wie folgt vor:**

1. Fügen Sie dem DirectorySearch-Element (siehe Seite 58) in der Datei "directory.xml" für das CA IdentityMinder-Verzeichnis den folgenden Parameter hinzu:

   ```
   minsortrules="1"
   ```

   **Hinweis**: Weitere Informationen zum Ändern eines vorhandenen CA IdentityMinder-Verzeichnisses finden Sie unter Aktualisieren von Einstellungen für ein CA IdentityMinder-Verzeichnis (siehe Seite 187).

2. Legen Sie die folgenden Berechtigungen für die Datei "vlvcntrl.ldif" fest:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```
3. Importieren Sie wie folgt VLV-Suchdefinitionen und -Indexdefinitionen:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```
4. Halten Sie das Verzeichnis wie folgt an:
   ```
   stop-slapd
   ```
5. Erstellen Sie die Indizes mithilfe von "runvlvindex".
6. Starten Sie das Verzeichnis wie folgt:
   ```
   start-slapd
   ```

## Konfigurieren von Paging-Unterstützung für Active Directory

Um die Paging-Unterstützung in Active Directory zu konfigurieren, führen Sie die folgenden allgemeinen Schritte aus:

- Konfigurieren Sie die Unterstützung für Virtual List View (siehe Seite 100).
- Konfigurieren Sie "MaxPageSize" für Active Directory (siehe Seite 101). (**Nur für Verzeichnisse, die vor CA IdentityMinder r12.5 SP7 erstellt wurden**)

### Konfigurieren der Unterstützung für Virtual List View (VLV)

Active Directory unterstützt Virtual List View (VLV), eine Methode zum Zurückgeben von Suchergebnissen in einer bestimmten Reihenfolge oder in bestimmten Teilmengen. Diese Methode unterscheidet sich von der Simple Paged Results-Methode, von der CA IdentityMinder ausgeht.

Um VLV verwenden zu können, müssen Sie Berechtigungen festlegen und Indizes erstellen. CA IdentityMinder beinhaltet die folgenden Dateien, die Sie für die Paging-Unterstützung konfigurieren müssen:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Diese Dateien sind Teil des NeteAuto-Beispiels unter "samples\NeteAuto" in den Verwaltungstools.

Die Verwaltungstools werden in den folgenden Standardordnern installiert:

Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

**Gehen Sie wie folgt vor:**

1. Fügen Sie dem DirectorySearch-Element (siehe Seite 58) in der Datei "directory.xml" für das CA IdentityMinder-Verzeichnis den folgenden Parameter hinzu:

   ```
   minsortrules="1"
   ```

   **Hinweis**: Weitere Informationen zum Ändern eines vorhandenen CA IdentityMinder-Verzeichnisses finden Sie unter Aktualisieren von Einstellungen für ein CA IdentityMinder-Verzeichnis (siehe Seite 187).

2. Legen Sie die folgenden Berechtigungen für die Datei "vlvcntrl.ldif" fest:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importieren Sie wie folgt VLV-Suchdefinitionen und -Indexdefinitionen:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Halten Sie das Verzeichnis wie folgt an:
   ```
   stop-slapd
   ```

5. Erstellen Sie die Indizes mithilfe von "runvlvindex".

6. Starten Sie das Verzeichnis wie folgt:
   ```
   start-slapd
   ```

## Konfigurieren von "MaxPageSize" in Active Directory

Active Directory verwendet als Standardeinstellung für "MaxPageSize" den Wert "1000". Nehmen wir an, der Wert für das Attribut "maxpagesize" in der Datei "directory.xml" ist größer als oder gleich 1000. In diesem Fall zeigt CA IdentityMinder keine Warnung an, wenn die Anzahl der Suchergebnisse die maximale Zeilenanzahl in der Datei "directory.xml" überschreitet. Administratoren, die die Suche ausführen, wissen daher nicht, dass einige Suchergebnisse fehlen.

Um dieses Problem zu vermeiden, stellen Sie sicher, dass der Wert des Attributs "maxpagesize" für das Verzeichnis und jedes verwaltete Objekt kleiner ist als der Wert für "MaxPageSize" in Active Directory.

Nehmen Sie an, Sie erstellen ein CA IdentityMinder-Verzeichnis mithilfe der Vorlagendatei "directory.xml", die zusammen mit CA IdentityMinder 12.5 SP7 oder höher installiert wird. In diesem Fall müssen Sie keine zusätzlichen Schritte für die Paging-Unterstützung ausführen. Das Attribut "maxpagesize" in "directory.xml" wird standardmäßig festgelegt.

Wenn Sie jedoch einem vorhandenen CA IdentityMinder-Verzeichnis Paging-Unterstützung hinzufügen, muss das Attribut "maxpagesize" in "directory.xml" kleiner sein als 1000.

Wenn das Active Directory-Attribut "MaxPageSize" den Wert "1000" hat, müssen Sie darauf achten, dass Sie das Attribut "maxpagesize" für das CA IdentityMinder-Verzeichnis und alle verwalteten Objekte entsprechend festlegen.

# Kapitel 4: Verwaltung relationaler Datenbanken

Dieses Kapitel enthält folgende Themen:

CA IdentityMinder-Verzeichnisse (siehe Seite 103)
Wichtige Hinweise für die Konfiguration von CA IdentityMinder für relationale Datenbanken (siehe Seite 105)
Erstellen einer Oracle-Datenquelle für WebSphere (siehe Seite 106)
So erstellen Sie ein CA IdentityMinder-Verzeichnis (siehe Seite 107)
So erstellen Sie eine JDBC-Datenquelle (siehe Seite 107)
So erstellen Sie eine ODBC-Datenquelle für die Verwendung mit SiteMinder (siehe Seite 115)
So beschreiben Sie eine Datenbank in einer Verzeichniskonfigurationsdatei (siehe Seite 115)
Verbindung zum Benutzerverzeichnis (siehe Seite 138)
Bekannte Attribute für eine relationale Datenbank (siehe Seite 144)
So konfigurieren Sie selbstabonnierende Gruppen (siehe Seite 149)
Validierungsregeln (siehe Seite 151)
Organisationsverwaltung (siehe Seite 151)
So verbessern Sie die Leistung von Verzeichnissuchen (siehe Seite 154)

## CA IdentityMinder-Verzeichnisse

Ein *CA IdentityMinder-Verzeichnis* beschreibt, wie Objekte, z. B. Benutzer, Gruppen und (optional) Organisationen, im Benutzerspeicher gespeichert und in CA IdentityMinder dargestellt werden. Ein CA IdentityMinder-Verzeichnis ist einer oder mehreren CA IdentityMinder-Umgebungen zugeordnet.

Die folgende Abbildung zeigt die Beziehung zwischen einem CA IdentityMinder-Verzeichnis und einem Benutzerspeicher:

Benutzerdatenbank
tblUsers
Mitarbeiter-ID
Vorname
Nachname
E-Mail
Anmelde-ID
Alter
Geburtsdatum
tblAddress
Mitarbeiter-ID
Straße
Stadt
Bundesland
PLZ

Identity Manager-Verzeichnis
Benutzerobjekte
Tabellen:
tblUsers
tblAddress
Attribute:
Mitarbeiter-ID
Vorname
Nachname
E-Mail
Anmelde-ID
Straße
Stadt
Bundesland
PLZ

Benutzerdatenbank
tblUsers
Mitarbeiter-ID
Vorname
Nachname
E-Mail
Anmelde-ID
Alter
Geburtsdatum
Adresse
Stadt

Administrator-Verzeichnis
Benutzerobjekte
Tabellen:
tblUsers
Attribute:
Mitarbeiter-ID
Vorname
Nachname
E-Mail
Anmelde-ID

**Hinweis:** Einige Benutzerattribute in der Datenbank sind nicht Teil des CA IdentityMinder-Verzeichnisses. Sie werden daher von CA IdentityMinder nicht verwaltet.

# Wichtige Hinweise für die Konfiguration von CA IdentityMinder für relationale Datenbanken

Bevor Sie CA IdentityMinder für die Verwaltung einer relationalen Datenbank konfigurieren, müssen Sie sicherstellen, dass die Datenbank die folgenden Anforderungen erfüllt:

- Auf die Datenbank muss über einen JDBC-Treiber oder einen ODBC-Treiber (Open Database Connectivity) zugegriffen werden können (wenn CA IdentityMinder mit SiteMinder integriert ist). Der Treiber muss äußere Verknüpfungen unterstützen. Wenn mehr als zwei Tabellen verwendet werden, um ein verwaltetes Objekt darzustellen, muss der Treiber außerdem verschachtelte äußere Verknüpfungen unterstützen.

  **Hinweis:** Wenn der Treiber keine äußeren Verknüpfungen unterstützt, verwendet CA IdentityMinder beim Abfragen der Datenbank innere Verknüpfungen. Dies kann jedoch unerwartete Abfrageergebnisse zur Folge haben.

- Geben Sie jedes von CA IdentityMinder verwaltete Objekt eindeutig an, z. B. Benutzer, Gruppe oder Organisation (sofern unterstützt). Die eindeutige Kennung eines Benutzers kann zum Beispiel eine Anmelde-ID sein.

  **Hinweis:** Vergewissern Sie sich, dass die eindeutige Kennung in einer einzelnen Spalte gespeichert ist.

- CA IdentityMinder erfordert einige mehrwertige Attribute, die als eine begrenzte Liste in einer einzelnen Zelle oder in mehreren Zeilen in einer separaten Tabelle gespeichert werden können. In der folgenden tblGroupMembers-Tabelle sind zum Beispiel die Mitglieder einer Gruppe gespeichert:

| ID | Mitglieder |
|---|---|
| Research | dmason |
| Research | rsavory |
| Marketing | dmason |
| Marketing | awelch |

Die ID-Spalte enthält die eindeutige Kennung für eine Gruppe, und die Mitglieder-Spalte enthält die eindeutige Kennung für ein Gruppenmitglied. Zum Beispiel sind "dmason" und "rsavory" Mitglieder der Gruppe "Research". Wenn diese Gruppe um ein neues Mitglied erweitert wird, wird "tblGroupMembers" eine weitere Zeile hinzugefügt.

- Wenn Ihre Umgebung Organisationen beinhaltet, führen Sie den folgenden Schritt aus:
  - Bearbeiten Sie ein in CA IdentityMinder enthaltenes SQL-Skript, und führen Sie es in der Datenbank aus, um die Unterstützung für Organisationen zu konfigurieren (siehe Seite 152).
  - CA IdentityMinder erfordert eine übergeordnete Organisation, die als Stammorganisation bezeichnet wird. Alle anderen Organisationen beziehen sich auf diese Stammorganisation.

    Weitere Informationen zu Organisationsanforderungen finden Sie unter Organisationsverwaltung (siehe Seite 151).

## Erstellen einer Oracle-Datenquelle für WebSphere

**Gehen Sie wie folgt vor:**

1. Navigieren Sie in der WebSphere-Verwaltungskonsole zu dem JDBC-Anbieter, den Sie bei der Konfiguration des JDBC-Treiber erstellt haben.
2. Erstellen Sie eine Datenquelle mit den folgenden Eigenschaften, und klicken Sie auf "Anwenden":

   **Name:** User Store Data Source

   **JNDI-Name:** userstore

   **URL:** jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. Konfigurieren Sie einen neuen J2C-Authentifizierungsdateneintrag für die Benutzerspeicher-Datenquelle:
   a. Geben Sie folgende Eigenschaften ein:

      **Alias:** User Store

      **Benutzer-ID:** *username*

      **Kennwort:** *password*

      Dabei stehen *username* und *password* für den Benutzernamen und das Kennwort des Kontos, das Sie beim Erstellen der Datenbank angegeben haben.
   b. Klicken Sie auf "OK", und verwenden Sie dann die Navigationsverknüpfungen oben in dem Fenster, um zu der Datenquelle zurückzukehren, die Sie erstellen.

4. Wählen Sie den erstellten J2C-Authentifizierungsdateneintrag für den Benutzerspeicher aus dem Listenfeld in den folgenden Feldern aus:
   - Component-managed Authentication Alias (Komponentenverwalteter Authentifizierungsalias)
   - Container-managed Authentication Alias (Containerverwalteter Authentifizierungsalias)
5. Klicken Sie auf "OK", und speichern Sie dann die Konfiguration.

   **Hinweis:** Um zu überprüfen, ob die Datenquelle richtig konfiguriert ist, klicken Sie im Konfigurationsbildschirm für die Datenquelle auf "Verbindung testen". Wenn der Verbindungstest fehlschlägt, starten Sie WebSphere neu, und testen Sie die Verbindung erneut.

## So erstellen Sie ein CA IdentityMinder-Verzeichnis

**Gehen Sie wie folgt vor:**

1. Wenn Sie SiteMinder verwenden, wenden Sie das Richtlinienspeicherschema an, bevor Sie ein CA IdentityMinder-Verzeichnis erstellen.

   **Hinweis:** Weitere Informationen zu bestimmten Richtlinienspeicherschemen und deren Anwendung finden Sie im *Installationshandbuch*.
2. Wenn Sie SiteMinder verwenden, erstellen Sie eine ODBC-Datenquelle für die Verwendung mit SiteMinder (siehe Seite 115).
3. Erstellen Sie eine Datenquelle für die von CA IdentityMinder verwaltete Benutzerdatenbank.
4. Beschreiben Sie die Datenbank in CA IdentityMinder, indem Sie die Verzeichniskonfigurationsdatei (directory.xml) ändern. Weitere Informationen hierzu finden Sie unter So beschreiben Sie eine Datenbank in einer Verzeichniskonfigurationsdatei.
5. Importieren Sie in der Management-Konsole die Verzeichniskonfigurationsdatei, und erstellen Sie das Verzeichnis.

## So erstellen Sie eine JDBC-Datenquelle

CA IdentityMinder erfordert eine JDBC-Datenquelle auf dem Anwendungsserver, auf dem CA IdentityMinder installiert ist, um eine Verbindung zum Benutzerspeicher herstellen zu können. Die Anweisungen zum Erstellen einer Datenquelle unterscheiden sich je nach Anwendungsserver.

# Erstellen einer JDBC-Datenquelle für JBoss-Anwendungsserver

**Gehen Sie wie folgt vor:**

1. Erstellen Sie eine Kopie der folgenden Datei:

   *jboss_home*\server\default\deploy\objectstore-ds.xml

   *jboss home*

   Das Installationsverzeichnis des JBoss-Anwendungsservers, auf dem CA IdentityMinder installiert ist.

   Die neue Datei muss sich im gleichen Verzeichnis befinden.

2. Benennen Sie die Datei in "userstore-ds.xml" um.

3. Bearbeiten Sie die Datei "userstore-ds.xml" wie folgt:

   a. Suchen Sie das <jndi-name>-Element.

   b. Ändern Sie wie folgt den Wert des <jndi-name>-Elements von "jdbc/objectstore" in "userstore":

      <jndi-name>userstore</jndi-name>

   c. Ändern Sie wie folgt im <connection-url>-Element den Parameter "DatabaseName" in den Namen der Datenbank, die als Benutzerspeicher dient:

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      *ipaddress*

      Gibt die IP-Adresse des Rechners an, auf dem der Benutzerspeicher installiert ist.

      *port*

      Gibt die Portnummer für die Datenbank an.

      *userstore_name*

      Gibt den Namen der Datenbank an, die als Benutzerspeicher dient.

4. Führen Sie die folgenden Schritte aus, wenn Sie einen JBoss-Sicherheitsbereich erstellen möchten, was zur Unterstützung von FIPS erforderlich ist:

   a. Benennen Sie die Sicherheitsdomäne in "<security-domain>imuserstoredb</security-domain>" um.

   b. Speichern Sie die Datei.

   c. Überspringen Sie die restlichen Schritte. Führen Sie statt dessen die Schritte unter Verwenden eines JBoss-Sicherheitsbereichs für die JDBC-Datenquelle (siehe Seite 110) aus.

5. Nehmen Sie die folgenden zusätzlichen Änderungen an der Datei "userstore-ds.xml" vor:

   a. Ändern Sie den Wert des <user-name>-Elements in den Benutzernamen für ein Konto, das Lese- und Schreibzugriff auf den Benutzerspeicher hat.

   b. Ändern Sie den Wert des <password>-Elements in das Kennwort für das im <user-name>-Element angegebene Konto.

   **Hinweis**: Der Benutzername und das Kennwort werden in dieser Datei unverschlüsselt angezeigt. Sie können daher auch einen JBoss-Sicherheitsbereich erstellen, anstatt die Datei "userstore-ds.xml" zu bearbeiten.

6. Speichern Sie die Datei.

## Verwenden eines JBoss-Sicherheitsbereichs für die JDBC-Datenquelle

Stellen Sie sicher, dass Sie eine JDBC-Datenquelle auf einem JBoss-Anwendungsserver erstellen. Sie können die Datenquelle so konfigurieren, dass diese einen Benutzernamen und ein Kennwort verwendet oder dass sie einen Sicherheitsbereich verwendet.

**Wichtig**! Vergewissern Sie sich, dass Sie bei Verwendung von FIPS die Option für den JBoss-Sicherheitsbereich nutzen.

**Gehen Sie wie folgt vor:**

1. Führen Sie die Schritte unter Erstellen einer JDBC-Datenquelle für JBoss-Anwendungsserver (siehe Seite 108) aus.

   Geben Sie in der Datei "userstore-ds.xml" keinen Benutzernamen und kein Kennwort an, wie in Schritt 4 beschrieben.

2. Öffnen Sie die Datei "login-cfg.xml" im Verzeichnis "*jboss_home*\server\default\conf".

3. Suchen Sie den folgenden Eintrag in der Datei:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option
name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. Kopieren Sie den gesamten Eintrag, und fügen Sie ihn in die Datei "login-cfg.xml" zwischen den Tags <policy> und </policy> ein.

5. Nehmen Sie in dem Eintrag, den Sie in die Datei eingefügt haben, die folgenden Änderungen vor:

   a. Ändern Sie wie folgt den Wert des Namensattributs von "imobjectstoredb" in "imuserstoredb":

   ```
   <application-policy name="imuserstoredb">
   ```

   b. Geben Sie wie folgt den Namen des Benutzers für die Authentifizierung am Benutzerspeicher an:

   ```
   <module-option name="userName">user_store_user</module-option>
   ```

   c. Geben Sie wie folgt das Kennwort für den im vorherigen Schritt angegebenen Benutzer an:

```
<module-option name="password">user_store_user_password</module-option>
```

**Hinweis**: Um das Kennwort für den Benutzerspeicher zu verschlüsseln, verwenden Sie das Kennworttool (pwdtools), das zusammen mit CA IdentityMinder installiert wurde.

d. Geben Sie wie folgt im Element <module-option name="managedConnectionFactoryName"> den korrekten "jdbc.jca:name" an:

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. Speichern Sie die Datei.
7. Starten Sie den Anwendungsserver neu.

## Erstellen einer JDBC-Datenquelle für WebLogic

Sie erstellen die Datenquelle in der WebLogic-Verwaltungskonsole.

**Hinweis**: Ausführliche Informationen über WebLogic-Verbindungspools finden Sie in der Dokumentation zu Oracle WebLogic 11.

**Gehen Sie wie folgt vor:**

1. Erstellen Sie in der WebLogic-Verwaltungskonsole eine JDBC-Datenquelle mit den folgenden Parametern:

   **Name:** User Store Data Source

   **JNDI-Name:** userstore
2. Erstellen Sie den Verbindungspool für die Datenquelle mit den folgenden Informationen:

- Verwenden Sie für SQL Server 2005-Datenbanken die folgenden Werte:

  **URL:** jdbc:sqlserver://*db_systemName*:1433

  **Treiberklassenname:** com.microsoft.sqlserver.jdbc.SQLServerDriver

  **Eigenschaften:** user=*username*

  databaseName=*user store name*

  selectMethod=cursor

  **Kennwort:** *password*

- Verwenden Sie für Oracle-Datenbanken die folgenden Werte:

  **URL:** jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

  **Treiberklassenname:** oracle.jdbc.driver.OracleDriver

  **Eigenschaften:** user=*username*

  **Kennwort:** *password*

3. Legen Sie nach der Konfiguration als Ziel für den Pool die Serverinstanz *wl_server_name* fest.

   Überprüfen Sie nach der Bereitstellung des Pools in der Konsole, ob Fehler aufgetreten sind.

   **Hinweis:** Möglicherweise wird ein Fehler angezeigt, demzufolge für einen nicht vorhandenen Pool die Datenquelle nicht erstellt werden konnte. Um diesen Fehler zu beheben, starten Sie WebLogic neu.

## WebSphere-Datenquellen

In den folgenden Abschnitten wird beschrieben, wie Sie eine SQL- oder Oracle-Datenquelle für WebSphere-Anwendungsserver erstellen.

### Erstellen einer SQL Server-Datenquelle für WebSphere

**Gehen Sie wie folgt vor:**

1. Navigieren Sie in der WebSphere-Verwaltungskonsole zu dem JDBC-Anbieter, den Sie bei der Konfiguration des JDBC-Treiber erstellt haben.
2. Wählen Sie im Abschnitt "Weitere Eigenschaften" die Option "Datenquellen" aus.
3. Erstellen Sie eine Datenquelle mit den folgenden Eigenschaften, und klicken Sie auf "Anwenden":

   **Name:** User Store Data Source

   **JNDI-Name:** userstore

   **Datenbankname:** *userstore_name*

   **Servername:** *db_systemname*

4. Konfigurieren Sie die selectMethod-Eigenschaft wie folgt:
   a. Wählen Sie im Abschnitt "Weitere Eigenschaften" die Option "Benutzerdefinierte Eigenschaften" aus.
   b. Klicken Sie auf die benutzerdefinierte Eigenschaft "selectMethod".
   c. Geben Sie den folgenden Text in das Feld "Wert" ein:

      cursor

   d. Klicken Sie auf "OK", und verwenden Sie dann die Navigationsverknüpfungen oben in dem Fenster, um zu der Datenquelle zurückzukehren, die Sie erstellen.
5. Konfigurieren Sie einen neuen J2C-Authentifizierungsdateneintrag für die Benutzerspeicher-Datenquelle:
   a. Wählen Sie im Abschnitt für verknüpfte Elemente J2EE Connector Architecture-Authentifizierungsdateneinträge (J2C) aus.
   b. Klicken Sie auf "Neu".
   c. Geben Sie folgende Eigenschaften ein:

      **Alias:** User Store

      **Benutzer-ID:** *username*

      **Kennwort:** *password*

      Dabei stehen *username* und *password* für den Benutzernamen und das Kennwort des Kontos, das Sie beim Erstellen der Datenbank angegeben haben.

   d. Klicken Sie auf "OK", und verwenden Sie dann die Navigationsverknüpfungen oben in dem Fenster, um zu der Datenquelle zurückzukehren, die Sie erstellen.
6. Wählen Sie den erstellten J2C-Authentifizierungsdateneintrag für den Benutzerspeicher aus dem Listenfeld im Feld "Component-managed Authentication Alias" (Komponentenverwalteter Authentifizierungsalias) aus.
7. Klicken Sie auf "OK", und speichern Sie dann die Konfiguration.

   **Hinweis:** Um zu überprüfen, ob die Datenquelle richtig konfiguriert ist, klicken Sie im Konfigurationsbildschirm für die Datenquelle auf "Verbindung testen". Wenn der Verbindungstest fehlschlägt, starten Sie WebSphere neu, und testen Sie die Verbindung erneut.

## Erstellen einer Oracle-Datenquelle für WebSphere

**Gehen Sie wie folgt vor:**

1. Navigieren Sie in der WebSphere-Verwaltungskonsole zu dem JDBC-Anbieter, den Sie bei der Konfiguration des JDBC-Treiber erstellt haben.

2. Erstellen Sie eine Datenquelle mit den folgenden Eigenschaften, und klicken Sie auf "Anwenden":

   **Name:** User Store Data Source

   **JNDI-Name:** userstore

   **URL:** jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. Konfigurieren Sie einen neuen J2C-Authentifizierungsdateneintrag für die Benutzerspeicher-Datenquelle:

   a. Geben Sie folgende Eigenschaften ein:

      **Alias:** User Store

      **Benutzer-ID:** *username*

      **Kennwort:** *password*

      Dabei stehen *username* und *password* für den Benutzernamen und das Kennwort des Kontos, das Sie beim Erstellen der Datenbank angegeben haben.

   b. Klicken Sie auf "OK", und verwenden Sie dann die Navigationsverknüpfungen oben in dem Fenster, um zu der Datenquelle zurückzukehren, die Sie erstellen.

4. Wählen Sie den erstellten J2C-Authentifizierungsdateneintrag für den Benutzerspeicher aus dem Listenfeld in den folgenden Feldern aus:

   - Component-managed Authentication Alias (Komponentenverwalteter Authentifizierungsalias)

   - Container-managed Authentication Alias (Containerverwalteter Authentifizierungsalias)

5. Klicken Sie auf "OK", und speichern Sie dann die Konfiguration.

   **Hinweis:** Um zu überprüfen, ob die Datenquelle richtig konfiguriert ist, klicken Sie im Konfigurationsbildschirm für die Datenquelle auf "Verbindung testen". Wenn der Verbindungstest fehlschlägt, starten Sie WebSphere neu, und testen Sie die Verbindung erneut.

## So erstellen Sie eine ODBC-Datenquelle für die Verwendung mit SiteMinder

Wenn CA IdentityMinder und SiteMinder integriert sind, definieren Sie eine ODBC-Datenquelle auf dem SiteMinder-Rechner, der auf die Datenbank verweist. Notieren Sie den Namen der Datenquelle für die spätere Verwendung. Fahren Sie wie folgt fort:

- **Windows:** Konfigurieren Sie die ODBC-Datenquelle als ein System-DN. Anweisungen hierzu finden Sie in der Dokumentation zu Ihrem Windows-Betriebssystem.
- **UNIX:** Fügen Sie der Datei "system_odbc.ini" im Verzeichnis *policy_server_installation/db* einen Eintrag hinzu, der die Parameter für die ODBC-Datenquelle angibt.

## So beschreiben Sie eine Datenbank in einer Verzeichniskonfigurationsdatei

Um eine Datenbank verwalten zu können, muss CA IdentityMinder die Datenbankstruktur und den Datenbankinhalt erkennen. Zum Beschreiben der Datenbank in CA IdentityMinder erstellen Sie eine Verzeichniskonfigurationsdatei (directory.xml).

Die Verzeichniskonfigurationsdatei enthält einen oder mehrere der folgenden Abschnitte:

**Informationen zum CA IdentityMinder-Verzeichnis**

Enthält Information zu dem CA IdentityMinder-Verzeichnis, das CA IdentityMinder verwendet.

**Attributvalidierung**

Definiert die Validierungsregeln, die auf das CA IdentityMinder-Verzeichnis angewandt werden.

**Informationen zum Anbieter**

Beschreibt den Benutzerspeicher, den CA IdentityMinder verwaltet.

**Informationen zur Verzeichnissuche**

Ermöglicht Ihnen, anzugeben, wie CA IdentityMinder den Benutzerspeicher durchsucht.

**Benutzerobjekt** **(siehe Seite 118)**

Beschreibt, wie Benutzer im Benutzerspeicher gespeichert werden und wie sie in CA IdentityMinder dargestellt werden.

**Gruppenobjekt** **(siehe Seite 118)**

Beschreibt, wie Gruppen im Benutzerspeicher gespeichert werden und wie sie in CA IdentityMinder dargestellt werden.

**Organisationsobjekt** **(siehe Seite 118)**

Beschreibt, wie Organisationen gespeichert werden und wie sie in CA IdentityMinder dargestellt werden.

**Selbstabonnierende Gruppen**

Konfiguriert die Unterstützung für Gruppen, denen Self-Service-Benutzer beitreten können.

Das Verzeichnis, in dem Sie die Verwaltungstools für CA IdentityMinder installiert haben, enthält die folgende Vorlage einer Verzeichniskonfigurationsdatei für relationale Datenbanken:

*admin_tools*\directoryTemplates\RelationalDatabase\directory.xml

*admin_tools*

Definiert das Installationsverzeichnis der CA IdentityMinder-Verwaltungstools, wie in den folgenden Beispielen dargestellt:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

**Hinweis:** Die Vorlage der Verzeichniskonfigurationsdatei in "directoryTemplates\RelationalDatabase" ist für Umgebungen konfiguriert, die Organisationen unterstützen. Um eine Verzeichniskonfigurationsdatei für eine Umgebung anzuzeigen, die keine Organisationen einschließt, suchen Sie in der Datei "directory.xml" nach dem NeteAuto-Beispiel im Verzeichnis "*admin_tools*\samples\NeteAutoRDB\NoOrganization".

Kopieren Sie die Konfigurationsvorlage in ein neues Verzeichnis, oder speichern Sie sie unter einem anderen Namen, damit sie nicht überschrieben wird. Anschließend können Sie die Vorlage ändern, sodass sie Ihre Datenbankstruktur widerspiegelt.

In der Verzeichniskonfigurationsdatei gelten zwei wichtige Konventionen:

- ## - Kennzeichnet erforderliche Werte.

  Um alle erforderlichen Informationen anzugeben, suchen nach doppelten Rautenzeichen (##), und ersetzen Sie sie durch entsprechende Werte. Beispielweise kennzeichnet ##PASSWORD_HINT, dass Sie ein Attribut angeben müssen, in dem eine Frage gespeichert ist, die der Benutzer zum Erhalt eines temporären Kennworts beantworten muss, wenn er sein Kennwort vergessen hat.

- @ - Kennzeichnet Werte, die von CA IdentityMinder ausgefüllt werden. Diese Werte dürfen in der Verzeichniskonfigurationsdatei nicht geändert werden. CA IdentityMinder fordert Sie beim Import der Verzeichniskonfigurationsdatei auf, diese Werte anzugeben.

Bevor Sie die Verzeichniskonfigurationsdatei ändern, benötigen Sie die folgenden Informationen:

- Tabellennamen für die Benutzer-, Gruppen- und Organisationsobjekte (wenn Ihre Struktur Organisationen einschließt).
- Eine Liste von Attributen in Benutzer-, Gruppen- und Organisationsprofilen (wenn Ihre Struktur Organisationen einschließt).

## Ändern der Verzeichniskonfigurationsdatei

Führen Sie das folgende Verfahren aus, um die Verzeichniskonfigurationsdatei zu ändern.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie eine Verbindung zur Datenbank.
2. Geben Sie an, wie lange CA IdentityMinder ein Verzeichnis suchen soll, bevor die Suche beendet wird.
3. Definieren Sie die von CA IdentityMinder verwalteten Objekte (siehe Seite 118) für Benutzer und Gruppen.
4. Ändern Sie bekannte Attribute.

   Bekannte Attribute kennzeichnen besondere Attribute, wie das Kennwortattribut in CA IdentityMinder.
5. Konfigurieren Sie die Unterstützung für selbstabonnierende Gruppen.
6. Wenn Ihre Umgebung Organisationen einschließt, konfigurieren Sie die Unterstützung für Organisationen.

**Weitere Informationen:**

Beschreibung von verwalteten Objekten (siehe Seite 118)
Organisationsverwaltung (siehe Seite 151)
So konfigurieren Sie selbstabonnierende Gruppen (siehe Seite 149)
Bekannte Attribute für eine relationale Datenbank (siehe Seite 144)

# Beschreibung von verwalteten Objekten

In CA IdentityMinder verwalten Sie die folgenden Objekttypen, die Einträgen in einem Benutzerspeicher entsprechen:

- Benutzer - Stellt Benutzer in einem Unternehmen dar.
- Gruppen **-** Stellt Gruppen von Benutzern dar, die etwas gemein haben.
- (Optional) Organisationen - Stellt Geschäftsbereiche dar. Organisationen können Benutzer, Gruppen und andere Organisationen enthalten.

  **Hinweis:** Weitere Informationen zur Konfiguration von Organisationen finden Sie unter Organisationsverwaltung (siehe Seite 151).

Eine Objektbeschreibung enthält die folgenden Informationen:

- Informationen zu dem Objekt (siehe Seite 118), wie die Tabellen, in denen das Objekt gespeichert ist.
- Die Attribute, in denen Informationen zu einem Eintrag gespeichert sind (siehe Seite 123). Zum Beispiel ist im Attribut "pager" eine Pagernummer gespeichert.

**Wichtig!** Eine CA IdentityMinder-Umgebung unterstützt nur jeweils einen Typ von Benutzer-, Gruppen- und Organisationsobjekt.

## So beschreiben Sie ein verwaltetes Objekt

Ein verwaltetes Objekt wird beschrieben, indem Sie Objektinformation in den Abschnitten für Benutzerobjekt, Gruppenobjekt und Organisationsobjekt (wenn die Datenbank Organisationen einschließt) der Verzeichniskonfigurationsdatei angeben.

Jeder dieser Abschnitte enthält ein ImsManagedObject-Element, wie zum Beispiel der folgende Code:

```
<ImsManagedObject name="User" description="My Users">
```

Das ImsManagedObject-Element kann die folgenden Elemente enthalten:

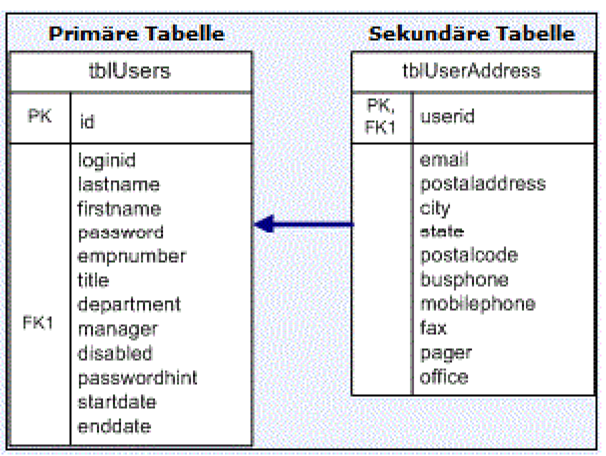
- Table (erforderlich)
- UniqueIdentifier (erforderlich)
- ImsManagedObjectAttr (erforderlich)
- RootOrg (nur für Organisationsobjekte)

## Datenbanktabellen

Verwenden Sie das Element "Table" in der Verzeichniskonfigurationsdatei, um die Tabellen zu definieren, in denen Informationen zu einem verwalteten Objekt gespeichert sind.

Jedes verwaltete Objekt muss eine primäre Tabelle aufweisen, die die eindeutige Kennung für das Objekt enthält. Zusatzinformationen können in sekundären Tabellen gespeichert werden.

Die folgende Abbildung zeigt einer Datenbank, bei der Benutzerinformationen in einer primären und sekundären Tabelle gespeichert sind:




Wenn die Informationen zu einem Objekt in mehreren Tabellen gespeichert sind, erstellen Sie ein Element "Table" für jede Tabelle. Verwenden Sie das Reference-Element in dem Table-Element für eine sekundäre Tabelle, um die Beziehung zur primären Tabelle zu definieren.

Wenn zum Beispiel grundlegende Informationen über einen Benutzer in "tblUsers" und Adressinformation in "tblUserAddress" gespeichert werden, würden die Tabellendefinitionen für das verwaltete Objekt "Benutzer" den folgenden Einträgen entsprechen:

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

## Tabellenelemente

Die Parameter für ein Tabellenelement lauten wie folgt:

**name**

(Erforderlich)

Gibt den Namen der Tabelle an, in der einige oder alle Attribute in einem verwalteten Profil eines Objekts gespeichert sind.

**primary**

Gibt an, ob die Tabelle die primäre Tabelle für das verwaltete Objekt ist. Die primäre Tabelle enthält wie folgt die eindeutige Kennung für das Objekt:

- True - Die Tabelle ist die primäre Tabelle.
- False - Die Tabelle ist eine sekundäre Tabelle (Standardeinstellung).

Wenn Sie den Parameter "primary" nicht angeben, geht CA IdentityMinder davon aus, dass die Tabelle eine sekundäre Tabelle ist.

**Hinweis:** Nur eine Tabelle kann die primäre Tabelle sein.

**Filter**

Gibt eine Teilmenge der Tabelleneinträge an, die sich auf das verwaltete Objekt beziehen.

Der optionale Filterparameter entspricht dem folgenden Beispiel:

```
filter="ORG=2"
```

**Hinweis:** Der Filter wird nur auf Abfragen angewandt, die CA IdentityMinder generiert. Wenn Sie eine generierte Abfrage mit einer benutzerdefinierten Abfrage überschreiben, geben Sie den Filter in der benutzerdefinierten Abfrage an.

**fullouterjoin**

Gibt an, ob die äußere Verknüpfung eine vollständige äußere Verknüpfung ist.

- True - Die äußere Verknüpfung ist eine vollständige äußere Verknüpfung. In diesem Fall ist die Bedingung, die zum Zurückgeben einer gültigen Zeile erforderlich ist,dass diese in beiden Tabellen der Verknüpfung zu finden ist.
- False - Die äußere Verknüpfung ist eine linke äußere Verknüpfung relativ zur primären Tabelle. In diesem Fall müssen nur die Zeilen in einer Tabelle in der Abfrage die Bedingung erfüllen (Standardeinstellung).

**Hinweis:** Die Parameter sind optional, wenn nichts anderes angegeben ist.

Der Parameter "Table" kann eines oder mehrere Reference-Elemente enthalten, um eine primäre Tabelle mit sekundären Tabellen zu verknüpfen.

## Reference-Element

Die Parameter im Reference-Element lauten wie folgt:

**childcol**

Gibt die Spalte in der sekundären Tabelle (im entsprechenden Table-Element) an, die der Spalte in der primären Tabelle zugeordnet ist.

**primarycol**

Gibt die Spalte in der primären Tabelle an, die der Spalte in der sekundären Tabelle zugeordnet ist.

**Hinweis:** Die Parameter sind optional, wenn nichts anderes angegeben ist.

## Angeben von Objektinformationen

Objektinformationen werden angegeben, indem Sie Werte für verschiedene Parameter festlegen.

**Gehen Sie wie folgt vor:**

1. Suchen Sie das ImsManagedObject-Element im Abschnitt für Benutzerobjekte, Gruppenobjekte oder Organisationsobjekte.
2. Geben Sie Werte für die folgenden Parameter an:

   **name**

   (Erforderlich)

   Gibt einen eindeutigen Namen für das verwaltete Objekt an.

   **Beschreibung**

   Gibt die Beschreibung des verwalteten Objekts an.

   **objecttype**

   (Erforderlich)

   Gibt den Typ des verwalteten Objekts an. Die folgenden Werte sind gültig:

   - USER
   - GROUP
   - ORGANIZATION

   Das ImsManagedObject-Element muss dem folgenden Code entsprechen:

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```
3. Geben Sie Tabelleninformationen an, wie unter Datenbanktabellen (siehe Seite 119) beschrieben.

4. Geben Sie die Spalte an, die die eindeutige Kennung für das Objekt (siehe Seite 122) enthält.
5. Beschreiben Sie die Attribute, die das Profil des Objekts bilden (siehe Seite 123).
6. Wenn Sie ein Organisationsobjekt konfigurieren, wechseln Sie zu Organisationsverwaltung (siehe Seite 151).

## So geben Sie die eindeutige Kennung für ein verwaltetes Objekt an

Jedes Objekt, das von CA IdentityMinder verwaltet wird, muss eine eindeutige Kennung haben. Vergewissern Sie sich, dass die eindeutige Kennung in einer einzelnen Spalte in der primären Tabelle des verwalteten Objekts gespeichert ist. Primäre Tabellen werden unter Datenbanktabellen (siehe Seite 119) beschrieben.

Verwenden Sie die Elemente "UniqueIdentifier" und "UniqueIdentifierAttr", um die eindeutige Kennung wie folgt zu definieren:

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

Das UniqueIdentifierAttr-Element erfordert den Namensparameter. Der Wert des Namensparameters ist das Attribut, in dem die eindeutige Kennung gespeichert ist. Der Wert kann ein physisches Attribut oder ein bekanntes Attribut (siehe Seite 79) sein.

Wenn Sie ein physisches Attribut angeben, beachten Sie die folgenden Punkte:

- Vergewissern Sie sich, dass das angegebene Attribut in der Datenbank vorhanden ist und dass es in der Verzeichniskonfigurationsdatei definiert ist, wie in So ändern Sie Attributbeschreibungen (siehe Seite 123) beschrieben. Geben Sie in der Attributbeschreibung die Berechtigung "nur lesen" oder "einmal schreiben" an, um zu verhindern, dass die eindeutige Kennung während einer Sitzung geändert wird.
- Verwenden Sie die folgende Syntax, um ein physisches Attribut anzugeben:

  *tablename.columnname*

  *tablename*

  Definiert den Namen der Tabelle, in der sich das Attribut befindet. Die angegebene Tabelle muss die primäre Tabelle sein.

  *columnname*

  Definiert den Namen der Spalte, in der das Attribut gespeichert ist.

- Wenn die Datenbank die eindeutige Kennung generiert, geben Sie einen benutzerdefinierten Vorgang für das Attribut (siehe Seite 134) an. Zum Beispiel können Sie einen Vorgang angeben, durch den die zuletzt generierte Kennung aus der Datenbank abgerufen wird.

## So ändern Sie Attributbeschreibungen

In einem Attribut werden Informationen zu einer Benutzer-, Gruppen- oder Organisationsentität gespeichert, wie eine Telefonnummer oder Adresse. Die Attribute einer Entität bestimmen deren Profil.

In der Verzeichniskonfigurationsdatei werden Attribute in ImsManagedObjectAttr-Elementen beschrieben. In den Abschnitten für Benutzer-, Gruppen- und Organisationsobjekte der Verzeichniskonfigurationsdatei:

- Ändern Sie die Standardattributbeschreibungen, um Ihre Datenbankattribute zu beschreiben.
- Erstellen Sie neue Attributbeschreibungen, indem Sie eine vorhandene Beschreibung kopieren und Werte nach Bedarf ändern.

Für jedes Attribut in Benutzer-, Gruppen- und Organisationsprofilen gibt es jeweils nur ein ImsManagedObjectAttr-Element. Zum Beispiel kann ein ImsManagedObjectAttr-Element eine Benutzer-ID beschreiben.

Ein ImsManagedObjectAttr-Element entspricht dem folgenden Code:

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

**Hinweis:** Wenn Sie eine Oracle-Datenbank verwenden, beachten Sie beim Konfigurieren von Attributen für verwaltete Objekte die folgenden Punkte:

- Oracle-Datenbanken beachten standardmäßig die Groß-/Kleinschreibung. Die Schreibweise der Attribute und Tabellennamen in der Verzeichniskonfigurationsdatei muss mit der Schreibweise der Attribute in Oracle übereinstimmen.

  Geben Sie für Zeichenfolgedatentypen eine maximale Länge an, um zu verhindern, dass diese abgeschnitten werden. Um die Länge von Zeichenfolgen zu beschränken, können Sie eine Validierungsregel erstellen, durch die ein Fehler angezeigt wird, wenn ein Benutzer eine Zeichenfolge eingibt, die die maximale Länge überschreitet.

Die ImsManagedObjectAttr-Parameter lauten wie folgt.

**Hinweis:** Die Parameter sind optional, wenn nichts anderes angegeben ist.

**physicalname**

(Erforderlich)

Gibt den physischen Namen des Attributs an, und muss eines der folgenden Details enthalten:

- Name und Verzeichnis, in dem der Wert gespeichert ist.

  Format: *tablename.columnname*

  Wenn zum Beispiel ein Attribut in der Spalte "id" der Tabelle "tblUsers" gespeichert ist, lautet der physische Name dieses Attributs wie folgt:

  tblUsers.id

  Sie müssen jede Tabelle, die ein Attribut enthält, in einem Table-Element (siehe Seite 119) definieren.

- Ein bekanntes Attribut.

  Ein bekanntes Attribut kann einen berechneten Wert darstellen. Sie können zum Beispiel ein bekanntes Attribut verwenden, um auf ein Attribut zu verweisen, das mithilfe eines benutzerdefinierten Vorgangs (siehe Seite 134) berechnet wurde.

**displayName**

(Erforderlich)

Gibt einen eindeutigen Namen für das Attribut an.

In der Benutzerkonsole wird der Anzeigename in der Liste der verfügbaren Attribute angezeigt, die einem Aufgabenfenster hinzugefügt werden können.

**Hinweis:** Sie dürfen den Anzeigenamen eines Attributs in der Verzeichniskonfigurationsdatei (directory.xml) nicht ändern. Um den Namen des Attributs in einem Aufgabenfenster zu ändern, geben Sie in der Aufgabenfensterdefinition eine Bezeichnung für das Attribut an. Weitere Informationen finden Sie im *Administrationshandbuch*.

**Beschreibung**

Gibt die Beschreibung des Attributs an.

**valuetype**

Gibt den Datentyp des Attributs an. Die folgenden Werte sind gültig:

**Zeichenfolge**

Der Wert kann eine beliebige Zeichenfolge sein.

Dies ist der Standardwert.

**Integer**

Der Wert muss eine Ganzzahl sein.

**Hinweis:** Der Parameter "Integer" unterstützt keine Dezimalzahlen.

**Number**

Der Wert muss eine Ganzzahl sein. Der Parameter "Number" unterstützt Dezimalzahlen.

**Datum**

Der Wert muss sich in ein gültiges Datum nach folgendem Muster auflösen lassen:

MM/TT/JJJJ

**ISODate**

Der Wert muss sich in ein gültiges Datum nach dem Muster JJJJ-MM-TT auflösen lassen.

**UnicenterDate**

Der Wert muss sich in ein gültiges Datum nach dem Muster JJJJJJJTTT auflösen lassen. Dabei gilt:

JJJJJJJ ist eine siebenstellige Darstellung des Jahres beginnend mit drei Nullen. Beispiel: 0002008

TTT ist eine dreistellige Darstellung des Tages beginnend mit Nullen, sofern erforderlich. Gültige Werte reichen von 001 bis 366.

Wenn der Werttyp eines Attributs falsch ist, können CA IdentityMinder-Abfragen fehlschlagen.

Um sicherzugehen, dass ein Attribut in der Datenbank korrekt gespeichert ist, können Sie ihm eine Validierungsregel zuordnen.

**required**

Gibt wie folgt an, ob zum Angeben des Attributs ein Wert erforderlich ist:

- True - Erforderlich
- False - Optional (Standardeinstellung)

**multi-valued**

Gibt wie folgt an, ob das Attribut mehrere Werte haben kann:

- True - Ein Attribut kann mehrere Werte haben.
- False - Ein Attribut kann nur einen Einzelwert haben (Standardeinstellung).

Das Gruppenmitgliedschaftsattribut in einem Benutzerprofil kann beispielsweise mehrere Werte haben, um die Gruppen zu speichern, denen ein Benutzer angehört.

Um Attribute mit mehreren Werten in einer begrenzten Liste anstelle in einer mehrzeiligen Tabelle zu speichern, müssen Sie das Trennzeichen im Parameter "delimiter" definieren.

Stellen Sie sicher, dass die Anzahl der möglichen Werte und die Länge jedes Wertes, den die Spalte zulässt, ausreichend sind.

**Wichtig!** Vergewissern Sie sich, dass das Gruppenmitgliedschaftsattribut in der Benutzerobjektdefinition mehrere Werte zulässt.

**wellknown**

Gibt den Namen des bekannten Attributs an.

Bekannte Attribute haben eine bestimmte Bedeutung in CA IdentityMinder.

Format: *%ATTRIBUTENAME%*

**Hinweis:** Wenn ein benutzerdefinierter Vorgang einem Attribut zugeordnet wird, müssen Sie ein bekanntes Attribut (siehe Seite 79) angeben.

**maxlength**

Bestimmt die maximale Größe der Spalte.

**permission**

Gibt wie folgt an, ob der Wert eines Attributs in einem Aufgabenfenster geändert werden kann:

**READONLY**

Der Wert wird angezeigt, kann aber nicht geändert werden.

**WRITEONCE**

Der Wert kann nicht mehr geändert werden, nachdem das Objekt erstellt wurde. Zum Beispiel kann eine Benutzer-ID nicht geändert werden, nachdem der Benutzer erstellt wurde.

**READWRITE**

Der Wert kann geändert werden (Standardeinstellung).

**hidden**

Gibt wie folgt an, ob ein Attribut in den CA IdentityMinder-Aufgabenfenstern angezeigt wird:

- True - Das Attribut wird den Benutzern nicht angezeigt.
- False - Das Attribut wird den Benutzern angezeigt (Standardeinstellung).

Logische Attribute verwenden verborgene Attribute.

**Hinweis:** Weitere Informationen zu logischen Attributen finden Sie im *Programmierhandbuch für Java*.

**system**

Nur CA IdentityMinder verwendet die Attribute. Gibt wie folgt an, dass Benutzer die Attribute in der Benutzerkonsole nicht ändern dürfen:

- True - Benutzer dürfen das Attribut nicht ändern. Das Attribut wird in der Benutzerkonsole nicht angezeigt.
- False - Benutzer können dieses Attribut ändern, und das Attribut kann Aufgabenfenstern in der Benutzerkonsole hinzugefügt werden (Standardeinstellung).

**validationruleset**

Ordnet dem Attribut einen Validierungsregelsatz zu.

Stellen Sie sicher, dass der angegebene Validierungsregelsatz in einem ValidationRuleSet-Element in der Verzeichniskonfigurationsdatei definiert ist.

**delimiter**

Definiert das Zeichen, durch das die Werte getrennt werden, wenn mehrere Werte in einer Spalte gespeichert werden.

**Wichtig!** Stellen Sie sicher, dass der Parameter "multivalued" auf "true" festgelegt ist, damit der Parameter "delimiter" angewandt wird.

**Hinweis:** Um zu verhindern, dass in der Benutzerkonsole vertrauliche Informationen angezeigt werden, wie Kennwörter oder Gehälter, können Sie den Parameter DataClassification (siehe Seite 74) angeben.

## Verwalten vertraulicher Attribute

CA IdentityMinder bietet die folgenden Methoden für die Verwaltung vertraulicher Attribute:

- Datenklassifizierungen für Attribute

  Mithilfe von Datenklassifizierungen können Sie Anzeige- und Verschlüsselungseigenschaften für Attribute in der Verzeichniskonfigurationsdatei (directory.xml) festlegen.

  Sie können Datenklassifizierungen, die vertrauliche Attribute verwalten, wie folgt definieren:

  - Zeigen Sie in den CA IdentityMinder-Aufgabenfenstern den Wert eines Attributs als Reihe von Sternchen an.

    Zum Beispiel können Sie Kennwörter als Sternchen anstelle von Klartext anzeigen.

  - Blenden Sie den Attributwert in den Fenstern "Gesendete Aufgaben anzeigen" aus.

    Mithilfe dieser Option können Sie Attribute ausblenden, damit Administratoren sie nicht sehen. Zum Beispiel können Gehaltsdetails wie die Höhe des Gehalts vor Administratoren verborgen werden, die den Aufgabenstatus in CA IdentityMinder anzeigen, aber keine Gehaltsdetails anzeigen müssen.

  - Ignorieren Sie bestimmte Attribute, wenn Sie eine Kopie eines vorhandenen Objekts erstellen.

  - Verschlüsseln von Attributen

- Feldtypen in Aufgabenprofilfenstern

  Wenn Sie ein Attribut nicht in der directory.xml-Datei ändern möchten, legen Sie die Anzeigeeigenschaft für das Attribut in den Bildschirmdefinitionen fest, in denen das vertrauliche Attribut angezeigt wird.

  Mithilfe des Feldtyps können Sie Attribute wie Kennwörter als Reihe von Sternchen anstelle von Klartext anzeigen.

  **Hinweis**: Weitere Informationen zum Feldtyp für vertrauliche Attribute finden Sie in den Abschnitten zu Feldtypen in der Benutzerkonsolen-Hilfe.

## Datenklassifizierungs-Attribute

Das Datenklassifizierungs-Element bietet eine Methode für das Zuordnen von zusätzlichen Eigenschaften zu einer Attributbeschreibung. Die Werte in diesem Element legen fest, wie CA IdentityMinder das Attribut verarbeitet. Dieses Element unterstützt die folgenden Parameter:

- sensitive

  Hat zur Folge, dass CA IdentityMinder das Attribut als Reihe von Sternchen (*) in den Fenstern "Gesendete Aufgaben anzeigen" anzeigt. Dieser Parameter verhindert, dass alte und neue Werte für das Attribut in den Fenstern "Gesendete Aufgaben anzeigen" als Klartext angezeigt werden.

  Wenn Sie eine Kopie eines vorhandenen Benutzers in der Benutzerkonsole erstellen, verhindert dieser Parameter außerdem, dass das Attribut zum neuen Benutzer kopiert wird.

- vst_hide

  Blendet das Attribut im Fenster "Ereignisdetails" auf der Registerkarte "Gesendete Aufgaben anzeigen" aus. Im Gegensatz zu vertraulichen Attributen, die als Sternchen angezeigt werden, werden vst_hidden-Attribute nicht angezeigt.

  Sie können diesen Parameter verwenden, damit Änderungen an einem Attribut, beispielsweise dem Gehalt, nicht im Fenster "Gesendete Aufgaben anzeigen" angezeigt werden.

- ignore_on_copy

  Hat zur Folge, dass CA IdentityMinder ein Attribut ignoriert, wenn ein Administrator eine Kopie eines Objekts in der Benutzerkonsole erstellt. Nehmen Sie zum Beispiel an, dass Sie ignore_on_copy für das Kennwortattribut eines Benutzerobjekts angegeben haben. Wenn Sie ein Benutzerprofil kopieren, überträgt CA IdentityMinder das Kennwort des aktuellen Benutzers nicht auf das neue Benutzerprofil.

- AttributeLevelEncrypt

  Verschlüsselt Attributwerte, wenn sie im Benutzerspeicher gespeichert werden. Wenn CA IdentityMinder für FIPS 140-2 aktiviert ist, verwendet CA IdentityMinder die RC2-Verschlüsselung oder die FIPS 140-2-Verschlüsselung.

  Weitere Informationen zur Unterstützung von FIPS 140-2 in CA IdentityMinder finden Sie im *Konfigurationshandbuch*.

  Die Attribute werden während Laufzeit als Klartext angezeigt.

  **Hinweis:** Um zu verhindern, dass Attribute in Fenstern als Klartext angezeigt werden, können Sie ein Element zu verschlüsselten Attributen hinzufügen, das sie als vertrauliche Daten klassifiziert. Weitere Informationen finden Sie unter Hinzufügen von Verschlüsselung auf Attributebene (siehe Seite 75).

- PreviouslyEncrypted

  Hat zur Folge, dass CA IdentityMinder alle verschlüsselte Werte im Attribut erkennt und entschlüsselt, wenn das Objekt im Benutzerspeicher aufgerufen wird.

  Mithilfe dieser Datenklassifizierung können Sie alle zuvor verschlüsselten Werte entschlüsseln.

  Der Klartextwert wird im Speicher gespeichert, wenn Sie das Objekt speichern.

## Konfigurieren von Datenklassifizierungs-Attributen

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei nach dem Attribut.
2. Fügen Sie das folgende Attribut nach der Attributbeschreibung hinzu:

   <DataClassification name="*parameter*">

   **parameter**

   Stellt einen der folgenden Parameter dar:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Eine Attributbeschreibung, die das Datenklassifizierungs-Attribut "vst_hide" enthält, entspricht zum Beispiel in etwa dem folgenden Code:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

## Verschlüsselung auf Attributebene

Sie können ein Attribut im Benutzerspeicher verschlüsseln, indem Sie eine AttributeLevelEncypt-Datenklassifizierung für dieses Attribut in der Verzeichniskonfigurationsdatei (directory.xml) angeben. Wenn die Verschlüsselung auf Attributebene aktiviert ist, verschlüsselt CA IdentityMinder den Wert dieses Attributs, bevor es im Benutzerspeicher gespeichert wird. Das Attribut wird in der Benutzerkonsole als Klartext angezeigt.

**Hinweis:** Um zu verhindern, dass Attribute in Fenstern als Klartext angezeigt werden, können Sie ein Element zu verschlüsselten Attributen hinzufügen, das sie als vertrauliche Daten klassifiziert. Weitere Informationen finden Sie unter Hinzufügen von Verschlüsselung auf Attributebene (siehe Seite 75).

Wenn die FIPS 140-2-Unterstützung aktiviert ist, wird das Attribut mithilfe der RC2-Verschlüsselung oder FIPS 140-2-Verschlüsselung verschlüsselt.

Beachten Sie Folgendes, bevor Sie die Verschlüsselung auf Attributebene implementieren:

- CA IdentityMinder kann bei einer Suche keine verschlüsselten Attribute finden.

  Nehmen Sie an, dass ein verschlüsseltes Attribut einer Mitglieds-, Admin- oder Eigentümerrichtlinie bzw. einer Identitätsrichtlinie hinzugefügt wird. CA IdentityMinder kann die Richtlinie nicht richtig auflösen, weil eine Suche nach dem Attribut nicht möglich ist.

  Ziehen Sie in Erwägung, das Attribut in der directory.xml-Datei auf searchable="false" festzulegen, zum Beispiel:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Wenn CA IdentityMinder einen gemeinsamen Benutzerspeicher und ein gemeinsames Bereitstellungsverzeichnis verwendet, verschlüsseln Sie nicht die Bereitstellungsserver-Attribute.

- Aktivieren Sie AttributeLevelEncrypt nicht für Benutzerkennwörter in Umgebungen, die den folgenden Kriterien entsprechen:

  - Umfassen eine CA SiteMinder-Integration und
  - Speichern Benutzer in einer relationalen Datenbank

  Wenn CA IdentityMinder mit CA SiteMinder integriert wird, führen verschlüsselte Kennwörter zu Problemen, wenn neue Benutzer versuchen, sich anzumelden, und Kennwörter als Klartext eingeben.

- Wenn Sie die Verschlüsselung auf Attributebene für einen Benutzerspeicher aktivieren, der von anderen Anwendungen als CA IdentityMinder verwendet wird, können die anderen Anwendungen das verschlüsselte Attribut nicht verwenden.

## Hinzufügen von Verschlüsselung auf Attributebene

Nehmen Sie an, dass Sie eine Verschlüsselung auf Attributebene für ein CA IdentityMinder-Verzeichnis hinzugefügt haben. CA IdentityMinder verschlüsselt automatisch vorhandene Klartext-Attributwerte, wenn Sie das Objekt speichern, das dem Attribut zugeordnet ist. Wenn Sie zum Beispiel das Kennwortattribut verschlüsseln, wird beim Speichern des Benutzerprofils das Kennwort verschlüsselt.

**Hinweis**: Um den Attributwert zu verschlüsseln, muss die Aufgabe, die Sie zum Speichern des Objekts verwenden, das Attribut einschließen. Um das Kennwortattribut im vorherigen Beispiel zu verschlüsseln, vergewissern Sie sich, dass das Kennwortfeld der Aufgabe hinzugefügt wird, die Sie zum Speichern des Objekts verwenden, zum Beispiel die Aufgabe "Benutzer ändern".

Alle neuen Objekte werden mit verschlüsselten Werten im Benutzerspeicher erstellt.

**Gehen Sie wie folgt vor:**

1. Führen Sie eine der folgenden Aufgaben aus:
   - Erstellen Sie ein CA IdentityMinder-Verzeichnis.
   - Aktualisieren Sie ein vorhandenes Verzeichnis, indem Sie die Verzeichniseinstellungen exportieren.
2. Fügen Sie dem Attribut, das Sie in der directory.xml-Datei verschlüsseln möchten, die folgenden Datenklassifizierungs-Attribute hinzu:

   **AttributeLevelEncrypt**

   Behalten Sie den Attributwert im Benutzerspeicher in verschlüsselter Form bei.

   **sensitive (optional)**

   Blendet den Attributwert in CA IdentityMinder-Fenstern aus. Ein Kennwort wird zum Beispiel als Reihe von Sternchen (*) angezeigt.

   Beispiel:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0" searchable="false">
   <DataClassification name="AttributeLevelEncrypt"/>
   <DataClassification name="sensitive"/>
   ```
3. Wenn Sie ein CA IdentityMinder-Verzeichnis erstellt haben, ordnen Sie das Verzeichnis einer Umgebung zu.
4. Um zu erzwingen, dass CA IdentityMinder alle Werte sofort verschlüsselt, ändern Sie alle Objekte mithilfe des Massendatenladers.

   **Hinweis**: Weitere Informationen zum Massendatenlader finden Sie im *Administrationshandbuch*.

## Entfernen der Verschlüsselung auf Attributebene

Wenn im CA IdentityMinder-Verzeichnis ein verschlüsseltes Attribut enthalten ist, dessen Wert als Klartext gespeichert ist, können Sie die AttributeLevelEncrypt-Datenklassifizierung entfernen.

Nachdem die Datenklassifizierung entfernt worden ist, werden die neuen Attributwerte in CA IdentityMinder nicht mehr verschlüsselt. Vorhandene Werte werden entschlüsselt, wenn Sie das Objekt speichern, das dem Attribut zugeordnet wird.

**Hinweis**: Um den Attributwert zu entschlüsseln, muss die Aufgabe, die Sie zum Speichern des Objekts verwenden, das Attribut einschließen. Um zum Beispiel ein Kennwort für einen vorhandenen Benutzer zu entschlüsseln, speichern Sie das Benutzerobjekt mit einer Aufgabe, die das Kennwortfeld enthält, beispielsweise die Aufgabe "Benutzer ändern".

Um zu erzwingen, dass CA IdentityMinder alle verschlüsselten Werte erkennt und entschlüsselt, die für das Attribut im Benutzerspeicher verbleiben, können Sie eine andere Datenklassifizierung, PreviouslyEncrypted, angeben. Der Klartextwert wird im Benutzerspeicher gespeichert, wenn Sie das Objekt speichern.

**Hinweis**: Durch die Datenklassifizierung "PreviouslyEncrypted" wird bei jedem Laden des Objekts der Verarbeitungsaufwand erhöht. Um Leistungsbeeinträchtigungen zu verhindern, können Sie die Datenklassifizierung "PreviouslyEncrypted" hinzufügen, jedes Objekt, dem dieses Attribut zugeordnet ist, laden und speichern und anschließend die Datenklassifizierung wieder entfernen. Mit dieser Methode werden alle gespeicherten verschlüsselten Werte automatisch in gespeicherten Klartext konvertiert.

**Gehen Sie wie folgt vor:**

1. Exportieren Sie die Verzeichniseinstellungen für das entsprechende CA IdentityMinder-Verzeichnis.
2. Entfernen Sie in der directory.xml-Datei die Datenklassifizierung "AttributeLevelEncrypt" für Attribute, die Sie entschlüsseln möchten.
3. Wenn Sie erzwingen möchten, dass CA IdentityMinder zuvor verschlüsselte Werte entfernt, fügen Sie das Datenklassifizierungs-Attribut "PreviouslyEncrypted" hinzu.

   Beispiel:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Um zu erzwingen, dass CA IdentityMinder alle Werte sofort entschlüsselt, ändern Sie alle Objekte mithilfe des Massendatenladers.

   **Hinweis**: Weitere Informationen zum Massendatenlader finden Sie im *Administrationshandbuch*.

## Benutzerdefinierte Vorgänge

Sie können für bestimmte verwaltete Objekte benutzerdefinierte Vorgänge definieren, um die folgenden Aufgaben auszuführen:

- Verwenden von gespeicherten Prozeduren
- Optimieren von Abfragen für die Datenbankstruktur
- Abrufen einer von der Datenbank generierten eindeutigen Kennung

Benutzerdefinierte Vorgänge werden nur auf Attribute angewandt.

Beachten Sie beim Angeben benutzerdefinierter Vorgänge die folgenden Punkte:

- Benutzer, die benutzerdefinierte Vorgänge angeben, müssen mit SQL vertraut sein.
- Benutzerdefinierte Vorgänge werden von CA IdentityMinder nicht validiert. Bis zur Laufzeit werden Syntaxfehler und ungültige Abfragen nicht gemeldet.
- Wenn Sie einen benutzerdefinierten Vorgang für ein Attribut angeben, können Sie dieses Attribut nicht in Suchfiltern in CA IdentityMinder-Aufgaben verwenden.
- Benutzerdefinierte Vorgänge müssen den XML-Standards entsprechen. Stellen Sie Sonderzeichen mithilfe von XML-Syntax dar. Geben Sie zum Beispiel ein einzelnes Anführungszeichen (’) als ' an.

Um einen benutzerdefinierten Vorgang anzugeben, verwenden Sie das Operation-Element.

## Operation-Element

Das Operation-Element definiert eine SQL-Anweisung, die eine benutzerdefinierte Abfrage ausführen oder eine gespeicherte Prozedur aufrufen kann, um ein Attribut zu erstellen, abzurufen, zu ändern oder zu löschen. Das Operation-Element ist ein Unterelement des IMSManagedObjectAttr-Elements, wie im folgenden Beispiel dargestellt:

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Die Parameter des Operation-Elements lauten wie folgt:

**name**

Gibt einen vordefinierten Namen für einen Vorgang an. Folgende Vorgänge sind gültig:

- Erstellen
- Get
- Festlegen
- Löschen
- GetDB

  Der GetDB-Vorgang ruft während der Erstellung eine eindeutige Kennung aus der Datenbank ab, wenn die eindeutige Kennung durch die Datenbank oder eine gespeicherte Prozedur generiert wird.

**value**

Definiert die SQL-Anweisung oder gespeicherte Prozedur, die ausgeführt werden soll. Die folgenden Werte sind gültig:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (für gespeicherte Prozeduren)

**Hinweis:** Die Parameter sind optional, wenn nichts anderes angegeben ist.

Das Operation-Element kann ein oder mehrere Parameter-Elemente enthalten.

## Parameter-Element

Ein Parameter-Element gibt Werte an, die an die Abfrage übergeben werden. Wenn mehrere Parameter-Elemente definiert werden, werden die Werte in der angegebenen Reihenfolge an die Abfrage übergeben.

Ein Parameter-Element erfordert den Parameter "name". Der Wert des Parameters "name" kann ein physisches Attribut oder ein bekanntes Attribut (siehe Seite 79) sein.

**Hinweis:** CA IdentityMinder muss die Werte erkennen, die im Parameter-Element an eine Abfrage übergeben werden. Der Wert kann zum Beispiel ein physischer Name oder ein bekanntes Attribut sein, das in den ImsManagedObjectAttr-Attributen definiert ist.

Wenn Sie ein physisches Attribut angeben, beachten Sie die folgenden Punkte:

- Verwenden Sie die folgende Syntax, um ein physisches Attribut anzugeben:

  *tablename.columnname*

  - *tablename*

    Gibt den Namen der Tabelle an, in der sich das Attribut befindet. Die angegebene Tabelle muss die primäre Tabelle sein.

  - *columnname*

    Gibt den Namen der Spalte an, in der das Attribut gespeichert ist.

- Das angegebene Attribut muss in der Datenbank vorhanden und in der Verzeichniskonfigurationsdatei definiert sein, wie in So ändern Sie Attributbeschreibungen (siehe Seite 123) beschrieben.

## Beispiel: Benutzerdefinierte Vorgänge für das Attribut "Business Number"

Im folgenden Beispiel wird das Attribut "Business Number" durch den Aufruf einer gespeicherten Prozedur generiert; es ist kein physisches Attribut in der Datenbank.

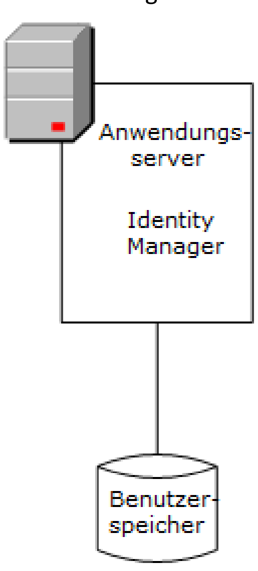
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

Beachten Sie Folgendes:

- "sp_getbusinessnumber", "sp_setbusinessnumber" und "sp_deletebusinessnumber" sind benutzerdefinierte gespeicherte Prozeduren.
- Der Wert, der vom Get-Vorgang zurückgegeben wird, wird dem Attribut %BUSINESS_NUMBER% zugeordnet.
- Das Fragezeichen (?) kennzeichnet Substitutionen, die zur Laufzeit vor Ausführung der Abfrage vorgenommen werden. Zum Beispiel wird im Get-Vorgang das bekannte Attribut %USER_ID% an die gespeicherte Prozedur "sp_getbusinessnumber" übergeben.

# Verbindung zum Benutzerverzeichnis

CA IdentityMinder stellt eine Verbindung zu einem Benutzerverzeichnis her, um Informationen, wie etwa zu Benutzer, Gruppe oder auch organisatorische Information, wie in der folgenden Darstellung angezeigt zu speichern:




Ein neues Verzeichnis oder eine neue Datenbank sind nicht erforderlich. Allerdings müssen das bestehende Verzeichnis oder die Datenbank auf einem System vorhanden sein, das einen vollständig qualifizierten Domänennamen besitzt (FQDN).

Eine Liste der unterstützten Verzeichnis- und Datenbanktypen finden Sie über die CA IdentityMinder-Support-Matrix auf der CA Support-Website.

Sie konfigurieren eine Verbindung zum Benutzerspeicher, wenn Sie ein CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen.

Wenn Sie die Verzeichniskonfiguration exportieren, nachdem Sie ein CA IdentityMinder-Verzeichnis erstellt haben, werden die Verbindungsinformationen zum Benutzerverzeichnis im Anbieter-Element der Verzeichniskonfigurationsdatei angezeigt.

## Beschreibung einer Datenbankverbindung

Um eine Datenbankverbindung zu beschreiben, verwenden Sie das Provider-Element und dessen Unterelemente in der Datei "directory.xml".

**Hinweis:** Wenn Sie ein CA IdentityMinder-Verzeichnis erstellen, müssen Sie keine Verzeichnisverbindungsinformationen in der Datei "directory.xml" angeben. Die Verbindungsinformationen werden im Assistenten für CA IdentityMinder-Verzeichnisse in der Management-Konsole angegeben.

Ändern Sie das Provider-Element nur für Aktualisierungen.

### Provider-Element

Das Provider-Element beinhaltet die folgenden Unterelemente:

**JDBC (erforderlich)**

Gibt die JDBC-Datenquelle an, die beim Herstellen einer Verbindung mit dem Benutzerspeicher verwendet wird. Geben Sie den JNDI-Namen an, den Sie beim Erstellen der JDBC-Datenquelle (siehe Seite 107) eingegeben haben.

**Credentials (erforderlich)**

Gibt den Benutzernamen und das Kennwort für den Zugriff auf die Datenbank an.

**DSN**

Gibt die ODBC-Datenquelle an, die beim Herstellen einer Verbindung mit dem Benutzerspeicher verwendet wird.

**Hinweis:** Dieses Unterelement wird nur bei Integration von CA IdentityMinder und SiteMinder angewandt. In CA IdentityMinder-Umgebungen, die SiteMinder nicht einschließen, wird dieses Unterelement ignoriert.

**SiteMinderQuery**

Gibt die benutzerdefinierten Abfrageschemen für die Suche nach Benutzerinformationen in einer relationalen Datenbank an.

**Hinweis:** Dieses Unterelement wird nur bei Integration von CA IdentityMinder und SiteMinder angewandt. In CA IdentityMinder-Umgebungen, die SiteMinder nicht einschließen, wird dieses Unterelement ignoriert.

Eine abgeschlossene Datenbankverbindung entspricht dem folgenden Beispiel:

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Die Attribute für das Provider-Element lauten wie folgt:

**type**

Gibt den Typ der Datenbank an. Geben Sie für Microsoft SQL Server- und Oracle-Datenbanken "RDB" an (Standardeinstellung).

**userdirectory**

Gibt den Namen der Benutzerverzeichnisverbindung an. Dieser Parameter entspricht dem Namen des Verbindungsobjekts, den Sie während der Erstellung des Verzeichnisses angegeben haben.

Wenn CA IdentityMinder und SiteMinder für Authentifizierungszwecke integriert sind, wird in SiteMinder eine Benutzerverzeichnisverbindung mit dem Namen erstellt, den Sie während der Installation für das Verbindungsobjekt angegeben haben. Wenn Sie eine Verbindung mit einem vorhandenen SiteMinder-Benutzerverzeichnis herstellen möchten, geben Sie an der Eingabeaufforderung für das Verbindungsobjekt den Namen dieses Benutzerverzeichnisses ein. CA IdentityMinder fügt den angegebenen Namen in den Parameter "userdirectory" ein.

Wenn CA IdentityMinder und SiteMinder nicht integriert sind, kann der Wert des Parameters "userdirectory" ein beliebiger Name sein, den Sie für die JDBC-Verbindung mit dem Benutzerspeicher festlegen.

**Hinweis:** Geben Sie keinen Namen für die Benutzerverzeichnisverbindung in der Datei "directory.xml" an. CA IdentityMinder fordert Sie während Erstellung des Verzeichnisses auf, den Namen anzugeben.

## Datenbankanmeldeinformationen

Um eine Verbindung mit der Datenbank herstellen zu können, muss CA IdentityMinder gültige Anmeldeinformationen an die Datenquelle übergeben. Die Anmeldeinformationen werden im Element "Credentials" definiert, das dem folgenden Beispiel entspricht:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Wenn Sie im Credentials-Element kein Kennwort angeben und versuchen, das CA IdentityMinder-Verzeichnis in der Management-Konsole zu erstellen, werden die Kennwortinformationen angefordert.

**Hinweis:** Es wird empfohlen, das Kennwort in der Management-Konsole anzugeben.

Wenn Sie das Kennwort in der Management-Konsole angeben, wird es von CA IdentityMinder verschlüsselt. Andernfalls sollten Sie das Kennwort mit dem Kennwort-Tool, das zusammen mit CA IdentityMinder installiert wird, verschlüsseln, sodass dieses nicht als unverschlüsselter Text angezeigt wird. Unter SiteMinder-Kennwörter finden Sie Anweisungen zur Verwendung des Kennworttools.

**Hinweis:** Sie können nur einen Satz von Anmeldeinformationen angeben. Wenn Sie mehrere Datenquellen definieren, müssen die angegebenen Anmeldeinformationen für alle Datenquellen gelten.

Die Parameter für Anmeldeinformationen lauten wie folgt:

**user**

Definiert den Anmelde-ID für ein Konto, das auf die Datenquelle zugreifen kann.

Geben Sie keinen Wert für den Parameter "user" in der Datei "directory.xml" an. CA IdentityMinder fordert Sie beim Erstellen des CA IdentityMinder-Verzeichnisses in der Management-Konsole zur Eingabe der Anmelde-ID auf.

**cleartext**

Gibt an, ob das Kennwort in der Datei "directory.xml" als unverschlüsselter Text angezeigt wird:

- True - Das Kennwort wird als unverschlüsselter Text angezeigt.
- False - Das Kennwort wird verschlüsselt (Standardeinstellung).

**Hinweis:** Diese Parameter sind optional.

## Data Source Name (DSN)

Das DSN-Element in der Datei "directory.xml" hat einen Parameter - den Namen der ODBC-Datenquelle, die CA IdentityMinder zum Herstellen einer Verbindung mit der Datenbank verwendet. Der Wert des Parameters "name" muss mit dem Namen einer vorhandenen Datenquelle übereinstimmen.

Hinweis: Dieses Element wird nur bei Integration von CA IdentityMinder und SiteMinder angewandt. Wenn CA IdentityMinder und SiteMinder nicht integriert sind, wird dieses Element ignoriert.

Wenn der Wert des Namensparameters "@SmDirDSN" lautet, müssen Sie keinen DSN-Namen in der Datei "directory.xml" angeben. CA IdentityMinder fordert Sie beim Import der Datei "directory.xml" auf, den DSN-Namen anzugeben.

Definieren Sie mehrere DSN-Elemente, um ein Failover zu konfigurieren. Wenn die primäre Datenquelle auf eine Anfrage nicht reagiert, wird die Anfrage von der nächsten definierten Datenquelle beantwortet.

Nehmen Sie zum Beispiel an, dass Sie das Failover wie folgt konfiguriert haben:

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA IdentityMinder verwendet die Datenquelle DSN1, um eine Verbindung mit der Datenbank herzustellen. Wenn ein Problem mit DSN1 besteht, versucht CA IdentityMinder, mithilfe von DSN2 eine Verbindung mit der Datenbank herzustellen.

**Hinweis:** Die Anmeldeinformationen, die Sie im Credentials-Element (siehe Seite 140) angeben, müssen für alle definierten DSNs gelten.

## SQL-Abfrageschemen

CA IdentityMinder verwendet Abfrageschemen, um Benutzer und Gruppeninformation in einer relationalen Datenbank zu suchen.

**Hinweis:** Dieses Element wird nur bei Integration von CA IdentityMinder und SiteMinder angewandt. In Umgebungen, die SiteMinder nicht einschließen, wird dieser Parameter ignoriert.

Wenn Sie ein CA IdentityMinder-Verzeichnis in der Management-Konsole erstellen, generiert CA IdentityMinder einen Satz von Abfrageschemen, die auf den erforderlichen Abfrageschemen in SiteMinder basieren. (Ausführliche Informationen über SiteMinder-Abfrageschemen finden Sie im *CA SiteMinder Web Access Manager Policy Server-Konfigurationshandbuch*.) Die Tabellen- und Spaltennamen in den SiteMinder-Abfrageschemen werden durch die Daten ersetzt, die Sie in der Verzeichniskonfigurationsdatei angeben.

### So definieren Sie benutzerdefinierte Abfrageschemen

Abfrageschemen werden in SiteMinderQuery-Elementen in der Verzeichniskonfigurationsdatei definiert. Ein SiteMinderQuery-Element entspricht dem folgenden Beispiel:

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

**Hinweis:** In der Beispielabfrage ist ' die XML-Syntax für das einzelne Anführungszeichen (’).

Das SiteMinderQuery-Element gilt nur, wenn CA IdentityMinder und SiteMinder integriert sind.

Die Parameter für Abfrageschemen lauten wie folgt:

**name**

Gibt den neudefinierten Namen eines SiteMinder-Abfrageschemas an.

Ändern Sie diesen Wert nicht.

**Abfrage**

Gibt die SQL-Anweisung oder gespeicherte Prozedur an, die ausgeführt werden soll. Die folgenden Werte sind gültig:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (für gespeicherte Prozeduren)

**Hinweis:** Diese Parameter sind für das SiteMinderQuery-Element erforderlich.

Bevor Sie Abfrageschemen anpassen, führen Sie die folgenden Schritte aus:

- Machen Sie sich mit den Standardabfrageschemen vertraut.

  **Hinweis:** Weitere Informationen zu den SQL-Abfrageschemen finden Sie im *CA SiteMinder Web Access Manager Policy Server-Konfigurationshandbuch*.

- Sammeln Sie umfassende Erfahrungen mit der Entwicklung von SQL-Abfragen.

## Ändern der Standardabfrageschemen

Führen Sie das folgende Verfahren aus, um die Standardabfrageschemen zu ändern.

**Gehen Sie wie folgt vor:**

1. Exportieren Sie die Verzeichniskonfigurationsdatei.

   CA IdentityMinder generiert eine Verzeichniskonfigurationsdatei, die alle aktuellen Einstellungen für das CA IdentityMinder-Verzeichnis enthält, einschließlich der generierten Abfrageschemen.

2. Speichern Sie die Verzeichniskonfigurationsdatei.

   **Hinweis:** Wenn Sie eine Sicherung der ursprünglichen Verzeichniskonfigurationsdatei erstellen möchten, speichern Sie die Datei unter einem anderen Namen oder in einem anderen Verzeichnis, bevor Sie die exportierte Datei speichern.

3. Suchen Sie das von CA IdentityMinder generierte Abfrageschema, das Sie ändern möchten.

4. Geben Sie in den Abfrageparameter das Abfrageschema oder die gespeicherte Prozedur ein, das bzw. die ausgeführt werden soll.

   **Hinweis:** Ändern Sie nicht den Abfragenamen.

5. Speichern Sie die Verzeichniskonfigurationsdatei, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

   Importieren Sie die Datei, um das CA IdentityMinder-Verzeichnis zu aktualisieren (siehe Seite 188).

# Bekannte Attribute für eine relationale Datenbank

Bekannte Attribute haben eine bestimmte Bedeutung in CA IdentityMinder. Sie werden durch die folgende Syntax gekennzeichnet:

*%ATTRIBUTENAME%*

In dieser Syntax muss *ATTRIBUTENAME* großgeschrieben werden.

Ein bekanntes Attribut wird mithilfe einer Attributbeschreibung (siehe Seite 123) einem physischem Attribut zugeordnet.

In der folgenden Attributbeschreibung wird das Attribut "tblUsers.password" dem bekannten Attribut %PASSWORD% zugeordnet, sodass CA IdentityMinder den Wert in "tblUsers.password" als ein Kennwort erkennt:

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Einige bekannte Attribute sind erforderlich; während andere optional sind.

## Bekannte Attribute für Benutzer

Die folgende Liste enthält bekannte Attribute für Benutzer:

**%ADMIN_ROLE_CONSTRAINT%**

Enthält eine Liste der Admin-Rollen (siehe Seite 148), die dem Administrator (siehe Seite 148) zugeordnet sind.

Das physische Attribut, das %ADMIN_ROLE_CONSTRAINT% zugeordnet ist, muss mehrere Werte zulassen, sodass es verschiedene Rollen aufnehmen kann.

Es wird empfohlen, das Attribut, das %ADMIN_ROLE_CONSTRAINT% zugeordnet ist, zu indizieren.

**%CERTIFICATION_STATUS%**

(Für die Verwendung der Benutzerzertifizierungsfunktion erforderlich.)

Enthält den Zertifizierungsstatus eines Benutzers.

**Hinweis**: Weitere Informationen zur Benutzerzertifizierung finden Sie im *Administrationshandbuch*.

**%DELEGATORS%**

Wird einer Liste mit Benutzern zugeordnet, die Arbeitselemente an den aktuellen Benutzer delegiert haben.

Dieses Attribut ist für die Verwendung der Delegierung erforderlich. Das physische Attribut, das %DELEGATORS% zugeordnet ist, muss mehrere Werte umfassen, und es muss Zeichenfolgen enthalten können.

**Wichtig!** Eine direkte Bearbeitung dieses Felds mit CA IdentityMinder-Aufgaben oder einem externen Tool hat beträchtliche Auswirkungen auf die Sicherheit.

**%EMAIL%**

(Für die Aktivierung der E-Mail-Benachrichtigungsfunktion erforderlich.)

Speichert die E-Mail-Adresse eines Benutzers.

**%ENABLED_STATE%**

(Erforderlich)

Verfolgt den Status eines Benutzers.

**Hinweis:** Der Datentyp des physischen Attributs, das %ENABLED_STATE% zugeordnet ist, muss "String" sein.

**%FIRST_NAME%**

Enthält den Vornamen eines Benutzers.

**%FULL_NAME%**

(Erforderlich)

Enthält den Vor- und Nachnamen eines Benutzers.

**%IDENTITY_POLICY%**

Enthält die Liste der Identitätsrichtlinien, die auf ein Benutzerkonto angewandt wurden.

CA IdentityMinder verwendet dieses Attribut, um zu bestimmen, ob eine Identitätsrichtlinie auf einen Benutzer angewandt werden muss. Wenn für die Richtlinie die Einstellung "Apply Once" (Einmal übernehmen) aktiviert ist und die Richtlinie im Attribut %IDENTITY_POLICY% aufgeführt ist, wendet CA IdentityMinder die Änderungen in der Richtlinie nicht auf den Benutzer an.

**Hinweis**: Weitere Informationen zu Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

**%LAST_CERTIFIED_DATE%**

(Für die Verwendung der Benutzerzertifizierungsfunktion erforderlich.)

Enthält das Datum, an dem die Rolle eines Benutzers zertifiziert wurde.

**Hinweis**: Weitere Informationen zur Benutzerzertifizierung finden Sie im *Administrationshandbuch*.

**%LAST_NAME%**

Enthält den Nachnamen eines Benutzers.

**%ORG_MEMBERSHIP%**

(Bei Unterstützung von Organisationen erforderlich.)

Enthält die eindeutige Kennung der Organisation, der der Benutzer angehört.

**%ORG_MEMBERSHIP_NAME%**

(Bei Unterstützung von Organisationen erforderlich.)

Enthält den benutzerfreundlichen Namen der Organisation, der der Benutzer angehört.

**%PASSWORD%**

Enthält ein Benutzerkennwort.

**Hinweis:** Der Wert des Attributs %PASSWORD% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%PASSWORD_DATA%**

(Für die Unterstützung von Kennwortrichtlinien erforderlich.)

Gibt das Attribut an, das Kennwortrichtlinieninformationen verfolgt.

**Hinweis:** Der Wert des Attributs %PASSWORD_DATA% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%PASSWORD_HINT%**

(Erforderlich)

Enthält eine vom Benutzer angegebene Frage und Antwort. Die Frage-/Antwortpaare werden im Fall eines vergessenen Kennworts verwendet.

**Hinweis:** Der Wert des Attributs %PASSWORD_HINT% wird in den CA IdentityMinder-Fenstern immer als eine Folge von Sternchen (*) angezeigt, sogar wenn für das Attribut oder Feld nicht festgelegt wurde, dass Kennwörter verborgen werden sollen.

**%USER_ID%**

(Erforderlich)

Speichert die Anmelde-ID eines Benutzers.

## Bekannte Attribute für Gruppen

Die folgende Liste enthält bekannte Attribute für Gruppen:

**%GROUP_ADMIN%**

Enthält die Administratoren einer Gruppe.

**Hinweis:** Das Attribut %GROUP_ADMIN% muss mehrere Werte zulassen.

**%GROUP_DESC%**

Enthält die Beschreibung einer Gruppe.

**%GROUP_ID%**

Enthält die eindeutige Kennung einer Gruppe.

**%GROUP_MEMBERSHIP%**

(Erforderlich)

Enthält eine Liste der Mitglieder einer Gruppe.

**Hinweis:** Das Attribut %GROUP_MEMBERSHIP% muss mehrere Werte zulassen.

**%GROUP_NAME%**

(Erforderlich)

Speichert den Namen einer Gruppe.

**%ORG_MEMBERSHIP%**

(Bei Unterstützung von Organisationen erforderlich.)

Enthält die eindeutige Kennung der Organisation, der die Gruppe angehört.

**%ORG_MEMBERSHIP_NAME%**

(Bei Unterstützung von Organisationen erforderlich.)

Enthält den benutzerfreundlichen Namen der Organisation, der die Gruppe angehört.

**%SELF_SUBSCRIBING%**

Bestimmt, ob Benutzer eine Gruppe abonnieren können.

## Attribut %Admin_Role_Constraint%

Wenn Sie eine Admin-Rolle erstellen, geben Sie eine oder mehrere Regeln für die Rollenmitgliedschaft an. Die Rolle wird allen Benutzern erteilt, die die Mitgliedschaftsregeln erfüllen. Wenn zum Beispiel die Mitgliedschaftsregel für die Rolle des Benutzer-Managers "title=User Manager" lautet, wird Benutzern mit dem Titel "User Manager" die Rolle "User Manager" erteilt.

**Hinweis**: Weitere Informationen zu Regeln finden Sie im *Administrationshandbuch*.

%ADMIN_ROLE_CONSTRAINT% ermöglicht es Ihnen, ein Profilattribut anzugeben, in dem alle Admin-Rollen eines Administrators gespeichert werden.

### So verwenden Sie das Attribut %ADMIN_ROLE_CONSTRAINT%

Um %ADMIN_ROLE_CONSTRAINT% als Einschränkung für alle Admin-Rollen zu verwenden, führen Sie die folgenden Schritte aus:

- Ordnen Sie das bekannte Attribut %ADMIN_ROLE_CONSTRAINT% einem mehrwertigen Profilattribut zu, um mehrere Rollen zu berücksichtigen.
- Wenn Sie eine Admin-Rolle in der CA IdentityMinder-Benutzeroberfläche konfigurieren, kann das folgende Szenario eine Einschränkung darstellen:

  Die Admin-Rollen stimmen mit dem *Rollennamen* überein.

  *role name*

  Definiert den Namen der Rolle, für die Sie die Einschränkung angeben.

  Beispiel: Admin-Rollen = User Manager

**Hinweis:** "Admin-Rollen" ist der Standardanzeigename für das Attribut %ADMIN_ROLE_CONSTRAINT%.

## Konfigurieren von bekannten Attributen

Führen Sie zum Konfigurieren bekannter Attribute die folgenden Schritte aus.

**Gehen Sie wie folgt vor:**

1. Suchen Sie in der Verzeichniskonfigurationsdatei nach dem folgenden Zeichen:

   ##

   Erforderliche Werte werden durch zwei Rautenzeichen (##) gekennzeichnet.

2. Ersetzen Sie den Wert, der mit ## beginnt, durch den physischen Namen des gewünschten Attributs, so wie es in der Datenbank enthalten ist. Geben Sie den Attributnamen im folgenden Format an:

   *tablename.columnname*

   Wenn zum Beispiel das Kennwortattribut in der Spalte "password" der Tabelle "tblUsers" gespeichert ist, geben Sie dies wie folgt an:

   ```
   tblUsers.password
   ```

3. Wiederholen Sie die Schritte 1 und 2, bis Sie alle erforderlichen Werte ersetzt und die gewünschten optionalen Werte eingefügt haben.

4. Ordnen Sie optional die bekannten Attribute physischen Attributen zu, sofern erforderlich.

5. Speichern Sie die Verzeichniskonfigurationsdatei.

# So konfigurieren Sie selbstabonnierende Gruppen

Um Self-Service-Benutzern den Beitritt zu Gruppen zu ermöglichen, können Sie in der Verzeichniskonfigurationsdatei die Unterstützung selbstabonnierender Gruppen konfigurieren.

**Gehen Sie wie folgt vor:**

1. Fügen Sie im Abschnitt für selbstabonnierende Gruppen das Element "SelfSubscribingGroups" wie folgt hinzu:

   ```
   <SelfSubscribingGroups type=search_type org=org_dn>
   ```

2. Geben Sie Werte für die folgenden Parameter ein:

   **type**

   Gibt an, wo CA IdentityMinder nach selbstabonnierenden Gruppen sucht. Die folgenden Werte sind gültig:

   - NONE - CA IdentityMinder sucht nicht nach Gruppen. Geben Sie NONE an, wenn Sie verhindern möchten, dass Benutzer selbst Gruppen abonnieren.
   - ALL - CA IdentityMinder durchsucht alle Gruppen im Benutzerspeicher. Geben Sie ALL an, wenn Benutzer alle Gruppen abonnieren können.
   - INDICATEDORG (*nur für Umgebungen, die Organisationen unterstützen*) - CA IdentityMinder sucht nach selbstabonnierenden Gruppen in der Organisation eines Benutzers und deren Unterorganisationen. Wenn zum Beispiel das Profil eines Benutzers der Marketingorganisation angehört, sucht CA IdentityMinder nach selbstabonnierenden Gruppen in der Marketingorganisation und in allen Unterorganisationen.
   - SPECIFICORG (*nur für Umgebungen, die Organisationen unterstützen*) - CA IdentityMinder sucht in einer bestimmten Organisation. Geben Sie die eindeutige Kennung der jeweiligen Organisation im Parameter "org" an.

   **org**

   Definiert die eindeutige Kennung der Organisation, in der CA IdentityMinder nach selbstabonnierenden Gruppen sucht.

   **Hinweis:** Stellen Sie sicher, dass Sie den Parameter "org" angeben, wenn "type=SPECIFICORG" festgelegt ist.

3. Starten Sie den SiteMinder-Richtlinienserver neu, wenn Sie eines der folgenden Elemente geändert haben:

   - Den Parameter "type" in oder von SPECIFICORG
   - Den Wert des Parameters "org"

Nachdem Sie die Unterstützung für selbstabonnierende Gruppen im CA IdentityMinder-Verzeichnis konfiguriert haben, können CA IdentityMinder-Administratoren angeben, welche Gruppen in der Benutzerkonsole selbstabonnierend sind.

Wenn sich ein Benutzer anmeldet, sucht CA IdentityMinder nach Gruppen in den angegebenen Organisationen und zeigt dem Benutzer die selbstabonnierenden Gruppen an.

# Validierungsregeln

Eine Validierungsregel setzt Anforderungen an Daten durch, die ein Benutzer in ein Feld des Aufgabenfensters eingibt. Die Anforderungen können einen Datentyp oder ein Format durchsetzen oder sicherstellen, dass die Daten im Kontext der anderen Daten im Aufgabenfenster gültig sind.

Validierungsregeln sind Profilattributen zugeordnet. Bevor eine Aufgabe verarbeitet wird, stellt CA IdentityMinder sicher, dass die für ein Profilattribut eingegebenen Daten alle zugeordneten Validierungsregeln erfüllen.

Sie können Validierungsregeln definieren und sie Profilattributen in der Verzeichniskonfigurationsdatei zuordnen.

# Organisationsverwaltung

Für relationale Datenbanken bietet CA IdentityMinder die Option, Organisationen zu verwalten. Wenn Ihre Datenbank Organisationen unterstützt, gilt Folgendes:

- Organisationen haben eine hierarchische Struktur.
- Alle verwalteten Objekte, wie Benutzer, Gruppen und andere Organisationen, gehören einer Organisation an.
- Wenn Sie eine Organisation löschen, werden alle Objekte, die dieser Organisation angehören, ebenfalls gelöscht.

Sie konfigurieren das Organisationsobjekt auf die gleiche Weise wie Benutzer- und Gruppenobjekte, jedoch mit einigen zusätzlichen Schritten.

## So richten Sie die Unterstützung von Organisationen ein

Führen Sie die folgenden Schritte aus, um die Unterstützung von Organisationen einzurichten:

1. Konfigurieren Sie die Unterstützung von Organisationen in der Datenbank (siehe Seite 152).
2. Beschreiben Sie das Organisationsobjekt in ImsManagedObject (siehe Seite 118).

   Stellen Sie sicher, dass Sie die Unterelemente "Table" und "UniqueIdentifier" konfigurieren.
3. Konfigurieren Sie die übergeordnete Organisation (siehe Seite 152).
4. Beschreiben Sie die Attribute (siehe Seite 123), die eine Organisation ausmachen.
5. Definieren Sie die bekannten Attribute für das Organisationsobjekt (siehe Seite 153).

## Konfigurieren der Unterstützung von Organisationen in der Datenbank

**Gehen Sie wie folgt vor:**

1. Öffnen Sie eines der folgenden SQL-Skripte in einem Editor:
   - Microsoft SQL Server-Datenbanken:

     ims_mssql_rdb.sql
   - Oracle-Datenbanken:

     ims_oracle_rdb.sql

     Diese Dateien sind in den folgenden Verzeichnissen gespeichert:

     *admin_tools*\directoryTemplates\RelationalDatabase

     *admin_tools* bezieht sich auf das Installationsverzeichnis der Verwaltungstools, die standardmäßig in einem der folgenden Verzeichnisse installiert werden:

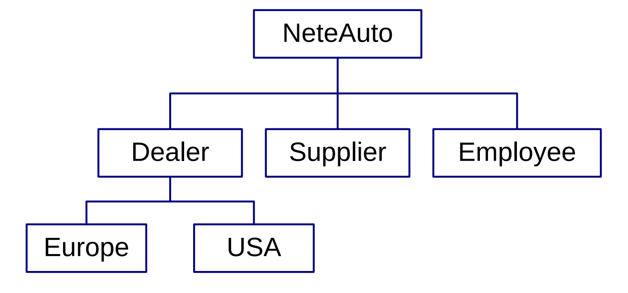
     **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools

     **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
2. Suchen Sie im SQL-Skript nach <@primary organization table@>, und ersetzen Sie den Eintrag durch den Namen der primären Tabelle für das Organisationsobjekt. Speichern Sie das SQL-Skript.
3. Führen Sie das SQL-Skript in der Datenbank aus.

## Spezifikation der Stammorganisation

Die Stammorganisation dient als übergeordnete Organisation im Verzeichnis. Alle Organisationen beziehen sich auf diese Stammorganisation.

In der folgenden Abbildung ist "NeteAuto" die Stammorganisation. Die anderen Organisationen sind Unterorganisationen von "NeteAuto":



Eine vollständige Definition der Stammorganisation entspricht dem folgenden Beispiel:

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

Nachdem Sie die grundlegenden Informationen für das Organisationsobjekt definiert haben, einschließlich der Tabellen, die das Organisationsprofil bilden, und der eindeutige Kennung des Organisationsobjekts, geben Sie die Stammorganisation in der Datei "directory.xml" an:

- Definieren Sie im Parameter "value" des RootOrg-Elements die Abfrage, die CA IdentityMinder zum Abrufen der Stammorganisation verwendet, wie im folgenden Beispiel dargestellt:

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- Geben Sie in den Parameter "name" des Result-Elements die eindeutige Kennung der Organisation ein, wie im folgenden Beispiel dargestellt:

  ```
  <Result name="%ORG_ID%" />
  ```

  **Hinweis:** Der Wert des Parameters "name" muss die eindeutige Kennung des Organisationsobjekts sein.

## Bekannte Attribute für Organisationen

Definieren Sie bekannte Attribute für die Attribute in einem Organisationsprofil, wie unter Bekannte Attribute (siehe Seite 79) beschrieben.

Die erforderlichen und optionalen bekannten Attribute für Organisationen lauten wie folgt:

**%ORG_DESCR%**

Enthält die Beschreibung einer Organisation.

**%ORG_MEMBERSHIP%**

(Erforderlich)

Enthält die übergeordnete Organisation einer Organisation.

**Hinweis:** Weitere Informationen zum Attribut %ORG_MEMBERSHIP% finden Sie unter "So definieren Sie die Organisationshierarchie".

**%ORG_MEMBERSHIP_NAME%**

(Erforderlich)

Enthält den benutzerfreundlichen Namen der übergeordneten Organisation (siehe Seite 154) einer Organisation.

**%ORG_NAME%**

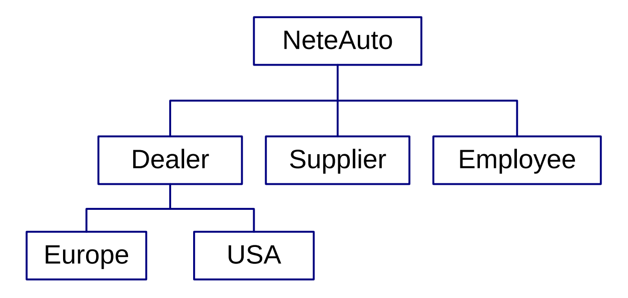
(Erforderlich)

Enthält den Namen der Organisation.

## So definieren Sie die Organisationshierarchie

Organisationen haben in CA IdentityMinder eine hierarchische Struktur, bestehend aus einer Stammorganisation und Unterorganisationen. Dabei können die Unterorganisationen weitere Unterorganisationen haben.

Jede Organisation mit Ausnahme der Stammorganisation hat eine übergeordnete Organisation. In der folgenden Abbildung ist zum Beispiel "Dealer" die übergeordnete Organisation für die Organisationen "USA" und "Europe":




Die eindeutige Kennung der übergeordneten Organisation wird in einem Attribut im Profil der Organisation gespeichert. Mithilfe der Informationen in diesem Attribut kann CA IdentityMinder die Organisationshierarchie erstellen.

Um das Attribut anzugeben, in dem die übergeordnete Organisation gespeichert ist, verwenden Sie die bekannten Attribute %ORG_MEMBERSHIP% und %ORG_MEMBERSHIP_NAME%, wobei das physische Attribut wie folgt den Namen der übergeordneten Organisation in einer Attributbeschreibung enthält:

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0" />
```

# So verbessern Sie die Leistung von Verzeichnissuchen

Um die Leistung von Verzeichnissuchen nach Benutzern, Organisationen und Gruppen zu verbessern, führen Sie die folgenden Schritte aus:

- Indizieren Sie die Attribute, die Administratoren in Suchanfragen angeben können.

- Überschreiben Sie die Standardeinstellung für das Verzeichniszeitlimit, indem Sie Werte für die Zeitlimitsuchparameter in einer Verzeichniskonfigurationsdatei (directory.xml) festlegen.
- Optimieren Sie das Benutzerverzeichnis. Weitere Informationen finden Sie in der Dokumentation zur verwendeten Datenbank.

Konfigurieren Sie datenbankspezifische Optionen in der ODBC-Datenquelle. Weitere Informationen finden Sie in der Dokumentation zur Datenquelle.

## So verbessern Sie die Leistung von großen Suchen

Wenn CA IdentityMinder einen großen Benutzerspeicher verwaltet, reicht bei Suchen, die viele Ergebnisse zurückgeben, der Systemspeicher möglicherweise nicht aus.

Die beiden folgenden Einstellungen bestimmen, wie CA IdentityMinder große Suchen verarbeitet:

- Maximale Zeilenanzahl

  Gibt die maximale Anzahl von Ergebnissen an, die CA IdentityMinder beim Durchsuchen eines Benutzerverzeichnisses zurückgeben kann. Wenn die Anzahl von Ergebnissen das Limit überschreitet, wird ein Fehler angezeigt.

- Seitengröße

  Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

  **Hinweis:** Wenn der Benutzerspeicher kein Paging unterstützt und ein Wert für "maxrows" angegeben wird, verwendet CA IdentityMinder nur den Wert für "maxrows" zum Steuern der Suchgröße.

Sie können die maximale Zeilenanzahl und Seitengröße an den folgenden Positionen konfigurieren:

- Benutzerspeicher

  In den meisten Benutzerspeichern und Datenbanken können Sie Beschränkungen für die Suche konfigurieren.

  **Hinweis:** Weitere Informationen finden Sie in der Dokumentation zu dem verwendeten Benutzerspeicher oder zu der verwendeten Datenbank.

- CA IdentityMinder-Verzeichnis

  Sie können das DirectorySearch-Element (siehe Seite 58) in der verwendeten Verzeichniskonfigurationsdatei (directory.xml) konfigurieren, um das CA IdentityMinder-Verzeichnis zu erstellen.

  Standardmäßig ist der Wert für die maximale Zeilenanzahl und Seitengröße für vorhandene Verzeichnisse unbegrenzt. Für neue Verzeichnisse ist der Wert für die maximale Zeilenanzahl unbegrenzt und der Wert für die Seitengröße ist 2000.

- Definition für verwaltete Objekte

  Um die maximale Zeilenanzahl und Seitengröße für einen einzelnen Objekttyp anstatt für ein ganzes Verzeichnis festzulegen, konfigurieren Sie die *Definition für verwaltete Objekte* (siehe Seite 61) in der Datei "directory.xml", die Sie zum Erstellen des CA IdentityMinder-Verzeichnisses verwenden.

  Das Festlegen von Beschränkungen für einen verwalteten Objekttyp ermöglicht es Ihnen, Anpassungen basierend auf den Geschäftsanforderungen vorzunehmen. Zum Beispiel haben die meisten Unternehmen mehr Benutzer als Gruppen. Diese Unternehmen können Beschränkungen nur für Benutzerobjektsuchen festlegen.

- Aufgabensuchfenster

  Sie können die Anzahl der Suchergebnisse steuern, die Benutzern in den Such- und Listenfenstern der Benutzerkonsole angezeigt werden. Wenn die Ergebnisanzahl die maximale Anzahl von Ergebnissen pro Seite überschreitet, die für die Aufgabe definiert ist, werden den Benutzer Links zu weiteren Ergebnisseiten angezeigt.

  Diese Einstellung wirkt sich nicht auf die Anzahl der Ergebnisse aus, die von einer Suche zurückgegeben werden.

  **Hinweis:** Weitere Informationen zum Festlegen der Seitengröße in Such- und Listenfenstern finden Sie im *Administrationshandbuch*.

Wenn die maximale Zeilenanzahl und Seitengröße an mehreren Positionen definiert werden, gilt die jeweils spezifischste Einstellung. Zum Beispiel haben Einstellungen für verwaltete Objekte Vorrang vor Einstellungen auf Verzeichnisebene.

# Kapitel 5: CA IdentityMinder-Verzeichnisse

Ein CA IdentityMinder-Verzeichnis gibt Informationen zu einem Benutzerverzeichnis an, das CA IdentityMinder verwaltet. Diese Informationen beschreiben, wie Objekte wie z. B. Benutzer, Gruppen und Organisationen im Benutzerspeicher gespeichert und in CA IdentityMinder angezeigt werden.

Sie können CA IdentityMinder-Verzeichnisse im CA IdentityMinder-Verzeichnisabschnitt der Management-Konsole erstellen, anzeigen, exportieren, aktualisieren und löschen.

**Hinweis:** Wenn CA IdentityMinder einen Cluster von SiteMinder-Richtlinienservern verwendet, halten Sie alle außer einen Richtlinienserver an, bevor Sie CA IdentityMinder-Verzeichnisse erstellen oder aktualisieren.

Dieses Kapitel enthält folgende Themen:


Voraussetzungen zum Erstellen eines CA IdentityMinder-Verzeichnisses (siehe Seite 157)
So erstellen Sie ein Verzeichnis (siehe Seite 158)
Erstellen von Verzeichnissen mithilfe des Verzeichniskonfigurations-Assistenten (siehe Seite 158)
Erstellen von Verzeichnissen mit einer XML-Konfigurationsdatei (siehe Seite 172)
Aktivieren von Bereitstellungsserver-Zugriff (siehe Seite 174)
Anzeigen von CA IdentityMinder-Verzeichnissen (siehe Seite 177)
CA IdentityMinder-Verzeichniseigenschaften (siehe Seite 178)
Aktualisieren von Einstellungen für ein CA IdentityMinder-Verzeichnis (siehe Seite 187)


## Voraussetzungen zum Erstellen eines CA IdentityMinder-Verzeichnisses

Bevor Sie ein CA IdentityMinder-Verzeichnis erstellen, müssen Sie folgende Schritte durchführen:

- Halten Sie alle außer einen CA IdentityMinder-Knoten an, bevor Sie ein CA IdentityMinder-Verzeichnis erstellen oder ändern.

  **Hinweis:** Wenn Sie einen Cluster von CA IdentityMinder-Knoten haben, kann nur ein CA IdentityMinder-Knoten aktiviert sein, wenn Sie Änderungen in der Management-Konsole vornehmen.

- Halten Sie alle außer einen Richtlinienserver an, bevor Sie CA IdentityMinder-Verzeichnisse erstellen oder aktualisieren.

  **Hinweis:** Wenn Sie einen Cluster von SiteMinder-Richtlinienservern haben, kann nur ein SiteMinder-Richtlinienserver aktiviert sein, wenn Sie Änderungen in der Management-Konsole vornehmen.

# So erstellen Sie ein Verzeichnis

In der Management-Konsole erstellen Sie ein CA IdentityMinder-Verzeichnis, das Struktur und Inhalt des Benutzerspeicher beschreibt, und das Bereitstellungsverzeichnis, das erforderliche Informationen für den Bereitstellungsserver speichert. Diese Verzeichnisse werden zur CA IdentityMinder-Umgebung zugeordnet.

Sie können eine der folgenden Methoden verwenden, um Verzeichnisse zu erstellen:

- Verwenden des Assistenten für Verzeichniskonfiguration

  Leitet Administratoren durch den Prozess, ein Verzeichnis für ihren Benutzerspeicher zu erstellen. Diese Methode hilft dabei, mögliche Konfigurationsfehler zu reduzieren.

  **Hinweis:** Verwenden Sie den Assistenten für Verzeichniskonfiguration nur, um neue Verzeichnisse für die LDAP-Benutzerspeicher zu erstellen. Um ein Verzeichnis für eine relationale Datenbank zu erstellen oder ein vorhandenes Verzeichnis zu aktualisieren, importieren Sie direkt eine directory.xml-Datei.

- Verwenden einer XML-Konfigurationsdatei

  Erlaubt Administratoren, eine vollständig konfigurierte XML-Datei auszuwählen, um den Benutzerspeicher oder Bereitstellungsserver zu erstellen oder zu ändern.

  Wählen Sie diese Methode aus, wenn Sie ein Verzeichnis für eine relationale Datenbank erstellen oder wenn Sie ein vorhandenes Verzeichnis aktualisieren.

**Weitere Informationen:**

Erstellen von Verzeichnissen mit einer XML-Konfigurationsdatei (siehe Seite 172)
Erstellen von Verzeichnissen mithilfe des Verzeichniskonfigurations-Assistenten (siehe Seite 158)

# Erstellen von Verzeichnissen mithilfe des Verzeichniskonfigurations-Assistenten

Der Verzeichniskonfigurations-Assistent leitet Administratoren durch den Prozess zum Erstellen eines Verzeichnisses für ihren Benutzerspeicher und reduziert Konfigurationsfehler. Bevor Sie den Assistenten starten, müssen Sie zunächst die Konfigurationsvorlage für das CA IdentityMinder-LDAP-Verzeichnis hochladen. Diese Vorlagen sind mit bekannten und erforderlichen Attributen vorkonfiguriert. Nach dem Eingeben von Verbindungsdetails für Ihren LDAP-Benutzerspeicher oder das Bereitstellungsverzeichnis können Sie LDAP-Attribute auswählen, bekannte Attribute verbinden und Metadaten für die Attribute eingeben. Wenn Sie die Attribute verbunden haben, klicken Sie auf "Fertig stellen", um das Verzeichnis zu erstellen.

## Starten des Verzeichniskonfigurations-Assistenten

Über den Verzeichniskonfigurations-Assistenten können Administratoren eine CA IdentityMinder-Vorlage auswählen und diese Vorlage für die Verwendung in der eigenen Umgebung ändern.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Directories" (Verzeichnisse), und wählen Sie "Create from Wizard" (Über Assistenten erstellen) aus.

   Sie werden aufgefordert, eine Verzeichniskonfigurationsdatei auszuwählen, um den Benutzerspeicher zu konfigurieren.

2. Klicken Sie auf "Durchsuchen", um die Konfigurationsdatei, mit der der Benutzerspeicher oder der Bereitstellungsserver konfiguriert wird, im folgenden Standardverzeichnis auszuwählen, und klicken Sie auf "Weiter".

   ```
   admin_tools\directoryTemplates\directory\
   ```

   **Hinweis:** "admin_tools" bezeichnet das Verzeichnis, in dem die Verwaltungstools installiert sind, und "directory" gibt den Namen des LDAP-Anbieters an.

   Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

   - Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

3. Geben Sie im Fenster "Verbindungsdetails" die Verbindungsinformationen für das LDAP-Verzeichnis oder den Bereitstellungsserver, die Verzeichnissuchparameter und Failover-Verbindungsinformationen an, und klicken Sie auf "Weiter".

4. Legen Sie im Fenster "Configure Managed Object" (Verwaltetes Objekt konfigurieren) die zu konfigurierenden Objekte fest, und klicken Sie auf "Weiter". Zur Auswahl stehen folgende Objekte:

   ■ Konfigurieren des verwalteten Objekts der Benutzer

   ■ Configure Group Managed Object (Auf Gruppenebene verwaltetes Objekt konfigurieren)

   ■ Configure Organization Object (Organisationsobjekt konfigurieren)

   ■ Show summary and deploy directory (Zusammenfassung anzeigen und Verzeichnis bereitstellen)

     **Hinweis:** Wählen Sie "Show summary and deploy directory" nur aus, wenn Sie die Konfiguration des Verzeichnisses abgeschlossen haben.

   a. Zeigen Sie die strukturellen und zusätzlichen Klassen im Fenster "Attribut auswählen" an, und ändern Sie sie ggf. Klicken Sie anschließend auf "Weiter".

   b. Verbinden Sie im Fenster "Select Attributes: Mapping Well-Knowns" (Attribut auswählen: bekannte Attribute verbinden) die bekannten CA IdentityMinder-Aliasnamen mit ausgewählten LDAP-Attributen, und klicken Sie auf "Weiter".

   c. (Optional) Zeigen Sie die Attributdefinitionen im Fenster "Describe User Attributes" (Benutzerattribute beschreiben) an, und ändern Sie sie. Klicken Sie anschließend auf "Weiter". Sie können den Anzeigenamen und die Beschreibung ändern.

   d. (Optional) Definieren Sie im Fenster "User Attribute Details" (Benutzerattributdetails) die Metadaten für jedes ausgewählte Attribut, und klicken Sie auf "Weiter".

      Das Fenster "Managed Object Selection" (Auswahl des verwalteten Objekts) wird angezeigt.

      Um Gruppen oder Organisationen zu konfigurieren, wählen Sie das verwaltete Objekt aus, und klicken Sie auf "Weiter", um die Fenster "Attribute" für diese Objekte aufzurufen.

5. Wählen Sie "Show summary and deploy directory" (Zusammenfassung anzeigen und Verzeichnis bereitstellen) aus, und klicken Sie anschließend auf "Weiter".

   Das Bestätigungsfenster wird geöffnet.

6. Zeigen Sie die Details zum Verzeichnis an.

   Wenn Fehler aufgetreten sind, klicken Sie auf die Schaltfläche "Zurück", um die Änderungen in den entsprechenden Fenstern auszuführen. Klicken Sie auf "Fertig stellen", um die Änderungen zu übernehmen.

   CA IdentityMinder validiert die Konfiguration und erstellt das Verzeichnis. Anschließend kehren Sie zum Fenster "Verzeichnisse" zurück, in dem Sie das neue Verzeichnis anzeigen können.

## Bildschirm "Select Directory Template" (Verzeichnisvorlage auswählen)

Verwenden Sie dieses Fenster, um eine Verzeichnis-XML-Datei für LDAP auszuwählen und einen Benutzerspeicher oder Bereitstellungsserver zu konfigurieren.

Klicken Sie auf "Durchsuchen", um die Konfigurationsdatei, mit der der Benutzerspeicher oder der Bereitstellungsserver konfiguriert wird, im folgenden Standardverzeichnis auszuwählen:

```
admin_tools\directoryTemplates\directory\
```

**Hinweis:** "admin_tools" bezeichnet das Verzeichnis, in dem die Verwaltungstools installiert sind, und "directory" gibt den Namen des LDAP-Anbieters an.

Die Verwaltungstools werden in den folgenden Standardordnern gespeichert:

- Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Nachdem Sie die Verzeichnis-XML-Datei ausgewählt haben, klicken Sie auf "Weiter", um das Fenster "Verbindungsdetails" anzuzeigen.

## Fenster "Verbindungsdetails"

Verwenden Sie dieses Fenster, um die Konfigurationsanmeldeinformationen für Ihren Benutzerspeicher einzugeben. Sie können auch die Verzeichnissuchparameter eingeben und Failover-Verbindungen hinzufügen. Nachdem Sie die Verbindungsinformationen eingegeben haben, klicken Sie auf "Weiter", um die zu verwaltenden Objekte auszuwählen.

**Hinweis:** Die Felder, die auf diesem Fenster angezeigt werden, hängen vom Typ des Benutzerspeichers ab, und davon, ob Sie die Verbindung mithilfe des Assistenten für die Verzeichniskonfiguration herstellen oder eine XML-Datei direkt importieren.

Die folgenden Felder sind in diesem Fenster verfügbar:

**Name**

Gibt den Namen des Benutzerverzeichnisses an, mit dem Sie Verbindung aufnehmen.

**Beschreibung**

Gibt eine Beschreibung des Benutzerverzeichnisses an.

**Host**

Gibt den Hostnamen für den Computer an, wo sich der Benutzerspeicher befindet.

**Port**

Gibt den Port für den Computer an, wo sich der Benutzerspeicher befindet.

**User DN (Benutzer-DN)**

Gibt den Benutzerdomänennamen zum Zugriff auf den LDAP-Benutzerspeicher an.

**JDBC-Datenquellen-JNDI-Name**

Gibt den Namen einer vorhandenen JDBC-Datenquelle an, die CA IdentityMinder verwendet, um mit der Datenbank Verbindung aufzunehmen.

**Benutzername**

Gibt den Benutzernamen zum Zugriff auf den Provisioning-Server an.

**Hinweis:** Ausschließlich für Provisioning-Server.

**Domäne**

Gibt den Domänennamen zum Zugriff auf den Provisioning-Server an.

**Hinweis:** Ausschließlich für Provisioning-Server.

**Kennwort**

Gibt das Kennwort zum Zugriff auf den LDAP-Benutzerspeicher bzw. den Provisioning-Server an.

**Kennwort bestätigen**

Bestätigt das Kennwort zum Zugriff auf den LDAP-Benutzerspeicher bzw. den Provisioning-Server.

**Sichere Verbindung**

Bei Auswahl wird eine Secure Sockets Layer (SSL) Verbindung zum LDAP-Benutzerverzeichnis erzwungen.

**Suchstamm**

Gibt den Speicherort in einem LDAP-Verzeichnis an, das als Ausgangspunkt für das Verzeichnis dient. Üblicherweise ist dies eine Organisation (O) oder eine Organisationseinheit (OU).

**Hinweis:** Ausschließlich für die LDAP-Benutzerspeicher.

**Search Maximum Rows (Maximale Such-Zeilen)**

Gibt die maximale Anzahl von Ergebnissen an, die CA IdentityMinder beim Durchsuchen eines Benutzerverzeichnisses zurückgeben kann. Wenn die Anzahl von Ergebnissen das Limit überschreitet, wird ein Fehler angezeigt.

Das Einstellen der maximalen Zeilenanzahl kann die Einstellungen im LDAP-Verzeichnis überschreiben, die Suchergebnisse beschränken. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Search Page Size (Suchseiten-Größe)**

Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

Beachten Sie die folgenden Aspekte beim Angeben der Suchseiten-Größe:

- Damit Sie die Option zur Festlegung der Seitengröße von Suchen verwenden können, muss der von CA IdentityMinder verwaltete Benutzerspeicher Paging unterstützen. Einige Benutzerspeichertypen können zusätzliche Konfiguration erfordern, um Paging zu unterstützen. Weitere Informationen finden Sie im *Konfigurationshandbuch*.
- Wenn der Benutzerspeicher kein Paging unterstützt und ein Wert für die maximalen Such-Zeilen angegeben wird, verwendet CA IdentityMinder nur den Wert für die maximalen Such-Zeilen, um die Suchgröße zu steuern.

**Such-Zeitlimit**

Gibt die Höchstzahl an Sekunden an, die CA IdentityMinder in einem Verzeichnis sucht, bevor es die Suche beendet.

**Failover-Host**

Gibt den Hostnamen des Systems an, in dem ein redundanter Benutzerspeicher oder ein alternativer Provisioning-Server vorhanden ist, falls das Primärsystem nicht verfügbar ist. Wenn mehrere Server aufgelistet sind, versucht CA IdentityMinder eine Verbindung zu den Systemen in der gleichen aufgelisteten Reihenfolge herzustellen.

**Failover-Port**

Gibt den Port des Systems an, in dem ein redundanter Benutzerspeicher oder ein alternativer Provisioning-Server vorhanden ist, falls das Primärsystem nicht verfügbar ist. Wenn mehrere Server aufgelistet sind, versucht CA IdentityMinder eine Verbindung zu den Systemen in der gleichen aufgelisteten Reihenfolge herzustellen.

**Schaltfläche "Hinzufügen"**

Klicken Sie hier, um zusätzliche Failover-Hostnamen und Portnummern hinzuzufügen.

## Konfigurieren des Fensters der verwalteten Objekte

Verwenden Sie dieses Fenster, um ein zu konfigurierendes Objekt auszuwählen.

Die folgende Liste steht für die Felder in diesem Fenster:

**Konfigurieren des verwalteten Objekts der Benutzer**

Beschreibt, wie Benutzer im Benutzerspeicher gespeichert werden und wie sie in CA IdentityMinder dargestellt werden.

**Configure Group Managed Object (Auf Gruppenebene verwaltetes Objekt konfigurieren)**

Beschreibt, wie Gruppen im Benutzerspeicher gespeichert werden und wie sie in CA IdentityMinder dargestellt werden.

**Configure Organization Managed Object (Auf Organisationsebene verwaltetes Objekt konfigurieren)**

Wenn der Benutzerspeicher Organisationen einschließt, wird hier beschrieben, wie Organisationen gespeichert und in CA IdentityMinder dargestellt werden.

**Show summary and deploy directory (Zusammenfassung anzeigen und Verzeichnis bereitstellen)**

Gibt an, dass alle verwalteten Objekte definiert wurden und Sie das Verzeichnis bereitstellen möchten. Nachdem Sie "Zusammenfassung anzeigen" ausgewählt haben und das Verzeichnis bereitstellen, klicken Sie "Weiter". Sie gelangen dann zu einer Übersichtsseite.

**Schaltfläche "Speichern"**

Klicken Sie hier, um Ihre xml-Datei zu speichern.

**Schaltfläche "Zurück"**

Klicken Sie hier, um zum Modifizieren zum Bildschirm "Verbindungsdetails" zurückzukehren.

**Schaltfläche "Weiter"**

Klicken Sie hier, um mit dem Bildschirm "Attribute auswählen" fortzufahren. Wählen Sie zum Konfigurieren den Benutzer, die Gruppe oder die Organisationsattribute.

## Bildschirm "Attribute auswählen"

Verwenden Sie dieses Fenster, um Struktur- oder Hilfsklassen für Ihren Benutzer, Ihre Gruppe oder Ihre Organisationsobjekte zu ändern oder hinzuzufügen. Dieses Fenster wird mit Werten vorkonfiguriert, die auf gebräuchlichen Verzeichnisschemen und auf Best Practices für den Verzeichnistyp basieren, den Sie verwenden. Ein Administrator kann die Strukturklasse ändern, indem er eine neue Klasse aus dem Drop-down-Menü auswählt. Beim Auswählen aktualisiert eine Klasse die Tabelle mit Attributen, die zur neuen Strukturklasse gehören.

Eine Hilfsklasse kann hinzugefügt werden, indem diese aus dem Drop-down-Menü ausgewählt wird. Beim Auswählen aktualisiert eine Klasse die Tabelle mit Attributen, die zur neuen Hilfsklasse gehören.

Die folgende Liste steht für die Felder, die auf diesem Bildschirm angezeigt werden:

**Struktureller Klassenname**

Gibt die Strukturklasse des zu konfigurierenden Attributs an.

**Änderungs-Schaltfläche**

Klicken Sie hier, um die Strukturklasse zu ändern.

**Auxiliary Class Name (Name der Hilfsklasse)**

Gibt die Hilfsklasse des zu konfigurierenden Attributs an.

**Schaltfläche "Hinzufügen"**

Klicken Sie hier, um eine zu konfigurierende Hilfsklasse hinzuzufügen.

**Objektklasse**

Gibt die Objektklasse des Containers an.

**ID**

Gibt die Container-ID an.

**Name**

Gibt den Namen des Containers an.

**Attribute-Tabelle**

Gibt den physischen Namen und die Objektklasse dahingehend an, ob das Attribut mit mehreren Werten ausgestattet ist. Außerdem gibt es den Datentyp der ausgewählten Attribute an. Attribute in dieser Tabelle können nach "Ausgewählt", "Objektklasse", "Mehrfachwerten" oder "Datentyp" sortiert werden.

**Schaltfläche "Zurück"**

Klicken Sie hier, um zum Bildschirm der konfigurierten verwalteten Objekte zurückzukehren.

**Weiter**

Klicken Sie hier, um mit dem Fenster der bekannten Zuordnungen fortzufahren und die erforderlichen und optionalen bekannten Aliase zuzuordnen.

## Fenster der bekannten Zuordnungen

Verwenden Sie dieses Fenster, um CA IdentityMinder bekannte Attribute zu ausgewählten LDAP-Attributen zuzuordnen. Ein Administrator kann in der Liste von bekannten Attributen (wenn sie für benutzerdefinierten Code erforderlich sind) Elemente hinzufügen, indem er ein neues bekanntes Attribut ins Textfeld eingibt und auf die Schaltfläche "Hinzufügen" klickt. Das Fenster wird aktualisiert, sodass Sie mit dem Hinzufügen beliebig vieler bekannter Attribute fortfahren können.

Die folgende Liste steht für die Felder, die auf diesem Bildschirm angezeigt werden:

**Erforderliche bekannte Attribute (Well-Knowns)**

Gibt die bekannten Attribute für Benutzer, Gruppen oder Organisationen an (wenn anwendbar), die für die Zuordnung zu den LDAP-Attributen erforderlich sind.

**Optionale Well-Knowns**

Gibt die bekannten Attribute für Benutzer, Gruppen oder Organisationen an (wenn anwendbar), die optional zugeordnet werden können.

**Neuer Well-Known**

Gibt ein bekanntes Attribut an, auf das über benutzerdefinierten Code verwiesen wird.

**Schaltfläche "Hinzufügen"**

Klicken Sie hier, um ein neues bekanntes Attribut zur Tabelle der optionalen Well-Knowns hinzuzufügen.

**Schaltfläche "Zurück"**

Klicken Sie hier, um zum Fenster der ausgewählten Benutzerattribute zurückzugehen und weitere Attribute auszuwählen. Die Zuordnungen, die Sie bereits vorgenommen haben, werden gespeichert und sind verfügbar, wenn Sie zu diesem Fenster zurückkehren.

**Schaltfläche "Weiter"**

Klicken Sie hier, um mit dem Fenster der grundlegenden Objektattribut-Definition fortzufahren und um grundlegende Attributdefinitionen anzugeben.

**Weitere Informationen**

Bekannte Attribute für einen LDAP-Benutzerspeicher (siehe Seite 79)
Bekannte Attribute für Gruppen (siehe Seite 83)
Bekannte Attribute für Benutzer (siehe Seite 80)
Bekannte Attribute zur Organisation (siehe Seite 85)

## Fenster der grundlegenden Objektattribut-Definition

Verwenden Sie dieses Fenster, um die in üblicher Weise festgelegten Definitionen anzuzeigen und zu ändern: Name und Beschreibung anzeigen.

Die folgende Liste steht für die Felder, die auf diesem Bildschirm angezeigt werden:

**Tabelle der verwalteten Objekte**

Gibt den Anzeigenamen, physischen Namen, bekannten Namen und die Beschreibung des verwalteten Objekts an. Verwenden Sie das Drop-down-Menü, um die Beschreibung bei Bedarf zu ändern. Sobald Sie die Änderungen vorgenommen haben, klicken Sie auf "Weiter", um fortzufahren.

**Schaltfläche "Zurück"**

Klicken Sie hier, um zum Fenster der bekannten Zuordnungen zurückzukehren und um die Details der Zuordnungen zu ändern.

**Schaltfläche "Weiter"**

Klicken Sie hier, um im Fenster "Detailed Object Attribute Definition Screen" (Detaillierte Objektattribut-Definition) fortzufahren, wo Sie zusätzliche Attributdefinitionen angeben können.

## Fenster "Detailed Object Attribute Definition Screen" (Detaillierte Objektattribut-Definition)

Verwenden Sie dieses Fenster, um weitere Attributdefinitionen anzugeben. Ein Administrator kann die Metadaten für jedes ausgewählte Attribut definieren, indem er den Anzeigenamen ändert und indem er das Attribut in den Benutzerkonsolen-Fenstern, den Datentyp des Wertes, die maximale Länge und den Validierungsregelsatz verwaltet. Sobald Sie die Attributdefinitionen angegeben haben, klicken Sie auf "Weiter", um fortzufahren.

Dieses Fenster enthält folgende Felder:

**Anzeigename**

Gibt den eindeutigen Namen für das verwaltete Objektattribut an. Dies ist der Name, der in der Benutzerkonsole angezeigt wird.

**Kennungen**

Gibt die Kennungen der Datenklassifizierung für den Wert des verwalteten Objektattributs an. Die Kennungen sind alle optional und standardgemäß auf "falsch" eingestellt; außer die für die Suche vorgesehenen. Die folgenden Kennungen können ausgewählt werden:

**erforderlich**

Zeigt an, dass das Attribut beim Erstellen von Objekten obligatorisch ist.

**Mehrere Werte**

Zeigt an, dass das Attribut mit mehreren Werten angezeigt wird.

**Ausgeblendet**

Zeigt an, dass das Attribut ausgeblendet wird.

**System**

Zeigt an, dass das Attribut ein Systemattribut ist und den Aufgabenfenstern nicht hinzugefügt wird.

**Durchsuchbar**

Zeigt an, dass das Attribut zu Suchfiltern hinzugefügt wird. Standardgemäß wahr.

**Sensible Verschlüsselung**

Zeigt an, dass das Attribut empfindlich ist. Es wird als eine Reihe von Sternchen (*) angezeigt.

**Ausgeblendet in VST**

Zeigt an, dass das Attribut im Fenster der Ereignisdetails zur Anzeige der gesendeten Aufgaben ausgeblendet wird.

**Nicht kopieren**

Zeigt an, dass das Attribut ignoriert werden muss, wenn ein Administrator die Kopie eines Objekts erstellt.

**Vormals verschlüsselt**

Zeigt an, dass das Attribut, auf das im Benutzerspeicher zugegriffen wird, vormals verschlüsselt war und dass eine Entschlüsselung erforderlich ist. Der eindeutige Textwert wird im Benutzerspeicher gesichert, wenn das Objekt gespeichert wird.

**Ungekennzeichnet verschlüsselt**

Zeigt an, dass das Attribut vormals im Benutzerspeicher verschlüsselt war und dass kein Kennungsname des Verschlüsselungsalgorithmus am Anfang des verschlüsselten Textes vorliegt.

**Datentyp**

Gibt den Datentyp des Wertes für das verwaltete Objektattribut in der Benutzerkonsole an. Zur Auswahl stehen folgende Komponenten:

- READONLY
- WRITEONCE
- READWRITE

**Maximum Length (Maximale Länge)**

Gibt die maximale Länge des Wertes für das verwaltete Objektattribut an

Standard: 0

**Validation Rule Set (Validierungsregelsatz)**

Gibt die Validierungsregelsätze an, um den Wert des verwalteten Objektattributs zu validieren. Zur Auswahl stehen folgende Komponenten:

- User Validation (Benutzervalidierung)
- Phone Format (Telefonformat)
- International Phone Format (Internationales Telefonformat)

**Schaltfläche "Zurück"**

Klicken Sie auf diese Schaltfläche, um zum Modifizieren zum Fenster der grundlegenden Objektattribut-Definitionen zurückzukehren.

**Schaltfläche "Weiter"**

Klicken Sie auf diese Schaltfläche, um mit dem Fenster zum Konfigurieren der verwalteten Objekte fortzufahren. In diesem Fenster können Sie das nächste zu konfigurierende verwaltete Objekt auswählen. Sobald Sie die verwalteten Objekte konfiguriert haben, wählen Sie die Anzeige-Zusammenfassung und das bereitstellte Verzeichnis, um Ihre Verzeichnisinformationen anzuzeigen und das Verzeichnis bereitzustellen.

**Weitere Informationen**

Verwalten vertraulicher Attribute (siehe Seite 71)

## Bestätigungs-Fenster

Dieses Fenster zeigt eine Zusammenfassung der Verzeichnis-Details an.

Die folgende Liste steht für die Felder, die auf diesem Bildschirm angezeigt werden:

**Verbindungs-Details**

Gibt die Verbindungsdetails für das Benutzerverzeichnis an.

**Details zu Benutzer/Gruppe/Organisation**

Gibt die Änderungen an, die am directory.xml vorgenommen werden.

**Schaltfläche "Zurück"**

Klicken Sie hier, um Details im Assistenten zu ändern.

**Schaltfläche "Speichern"**

Klicken Sie hier, um Ihre Auswahl zu speichern.

**Schaltfläche "Fertig stellen"**

Wenn alle Verzeichnisdetails richtig sind, klicken Sie hier, um den Assistenten zu verlassen.

Die Konfiguration wird validiert, und das Verzeichnis wird erstellt. Sie gelangen dann zurück zur Auflistungsseite der Verzeichnisse, wo das neue Verzeichnis aufgelistet wird. Um das neue Verzeichnis zu bearbeiten oder zu exportieren, wählen Sie es aus der Verzeichnisliste aus.

# Erstellen von Verzeichnissen mit einer XML-Konfigurationsdatei

Sie können ein CA IdentityMinder-Verzeichnis durch das Importieren einer vollständigen directory.xml-Datei in der Management-Konsole erstellen oder aktualisieren.

**Hinweis:** Wenn Sie ein Verzeichnis unter Verwendung einer directory.xml-Datei anstelle des Assistenten für Verzeichniskonfiguration erstellen, vergewissern Sie sich, dass Sie die Standardkonfigurationsvorlage geändert haben. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   http://*hostname*:*port*/iam/immanage

   ***Hostname***

   Definiert den voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist.

   ***port***

   Definiert die Portnummer des Anwendungsservers.

2. Klicken Sie auf "Directories" (Verzeichnisse).

   Das CA IdentityMinder-Verzeichnisfenster wird geöffnet.

3. Klicken Sie auf "Create or Update from XML" (Aus XML erstellen oder aktualisieren).

4. Geben Sie den Pfad und Dateinamen der Verzeichniskonfigurations-XML-Datei für das Erstellen des CA IdentityMinder-Verzeichnisses ein, oder suchen Sie nach der Datei. Klicken Sie auf "Weiter".

5. Geben Sie Werte für die Felder in diesem Fenster folgendermaßen an:

   **Hinweis:** Die Felder, die in diesem Fenster angezeigt werden, hängen vom Benutzerspeichertyp und der Information ab, die Sie in der Verzeichniskonfigurationsdatei in Schritt 4 angegeben haben. Wenn Sie Werte für eines dieser Felder in der Verzeichniskonfigurationsdatei angaben, fordert CA IdentityMinder Sie nicht auf, diese Werte erneut zu liefern.

   **Name**

   Bestimmt den Namen des CA IdentityMinder-Verzeichnisses, das Sie erstellen.

   **Beschreibung**

   (Optional) Beschreibt das CA IdentityMinder-Verzeichnis.

Connection Object Name (Name des Verbindungsobjekts)

Gibt den Namen des Benutzerverzeichnisses an, das das CA IdentityMinder-Verzeichnis beschreibt. Geben Sie *eins* der folgenden Details ein:

- Wenn CA IdentityMinder nicht in SiteMinder integriert ist, geben Sie einen aussagekräftigen Namen für das Objekt an, das CA IdentityMinder verwendet, um mit dem Benutzerspeicher Verbindung aufzunehmen.
- Wenn CA IdentityMinder in SiteMinder integriert ist und Sie ein Benutzerverzeichnis-Verbindungsobjekt in SiteMinder erstellen wollen, geben Sie einen aussagekräftigen Namen an. CA IdentityMinder erstellt das Benutzerverzeichnis-Verbindungsobjekt in SiteMinder mit dem Namen, den Sie angeben.
- Wenn CA IdentityMinder in SiteMinder integriert ist und Sie mit einem vorhandenen SiteMinder-Benutzerverzeichnis Verbindung aufnehmen wollen, geben Sie den Namen des SiteMinder-Benutzerverzeichnis-Verbindungsobjekts genau an, wie er in der Richtlinienserver-Benutzeroberfläche angezeigt wird.

**JDBC-Datenquellen-JNDI-Name (nur für relationale Verzeichnisse)**

Gibt den Namen einer vorhandenen JDBC-Datenquelle an, die CA IdentityMinder verwendet, um mit der Datenbank Verbindung aufzunehmen.

**Host (nur für LDAP-Verzeichnisse)**

Gibt den Hostnamen oder die IP-Adresse des Servers an, auf dem das Benutzerverzeichnis installiert ist.

Verwenden Sie für CA Directory-Benutzerspeicher den vollen Domänennamen des Hostsystems. Verwenden Sie nicht localhost.

Geben Sie für Active Directory-Benutzerspeicher den Domänennamen an, nicht die IP-Adresse.

**Port (nur für LDAP-Verzeichnisse)**

Gibt die Portnummer des Benutzerverzeichnisses an.

**Bereitstellungsdomäne**

Bereitstellungsdomäne, die CA IdentityMinder verwaltet.

**Hinweis:** Der Bereitstellungsdomänenname berücksichtigt Groß- und Kleinschreibung.

**Benutzername/Benutzer-DN**

Gibt den Benutzernamen für ein Konto an, das auf den Benutzerspeicher zugreifen kann.

Für Bereitstellungs-Benutzerspeicher muss das Benutzerkonto, das Sie angeben, das Domänenadministrator-Profil oder ein gleichwertiges Set von Berechtigungen für die Bereitstellungsdomäne haben.

**Kennwort**

Gibt das Kennwort für das Benutzerkonto an, das Sie im Benutzernamen (für relationale Datenbanken) oder Benutzer-DN-Feld angegeben haben (für LDAP-Verzeichnisse).

**Kennwort bestätigen**

Geben Sie das in das Feld "Kennwort" eingegebene Kennwort erneut zur Bestätigung ein.

**Sichere Verbindung (nur für LDAP-Verzeichnisse)**

Zeigt an, ob CA IdentityMinder eine sichere Verbindung verwendet.

Wählen Sie diese Option für Active Directory-Benutzerspeicher aus.

Klicken Sie auf "Weiter".

6. Überprüfen Sie die Einstellungen für das CA IdentityMinder-Verzeichnis. Klicken Sie auf "Fertig stellen", um das CA IdentityMinder-Verzeichnis mit den aktuellen Einstellungen zu erstellen, oder auf "Zurück", um es zu ändern.

   Statusinformationen werden im Verzeichniskonfigurations-Ausgabefenster angezeigt.

7. Klicken Sie zum Beenden auf "Fortfahren".

   CA IdentityMinder erstellt das Verzeichnis.

# Aktivieren von Bereitstellungsserver-Zugriff

Sie aktivieren den Zugriff auf den Bereitstellungsserver durch die Verwendung des Links "Directories" (Verzeichnisse) in der Management-Konsole.

**Hinweis**: Eine Voraussetzung für diesen Vorgang ist, das Bereitstellungsverzeichnis auf CA Directory zu installieren. Weitere Informationen dazu finden Sie im *Installationshandbuch*.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   `http://`*`hostname`*`:`*`port`*`/iam/immanage`

   *Hostname*

   Definiert den voll qualifizierten Hostnamen des Systems, auf dem der CA IdentityMinder-Server installiert ist.

   *port*

   Definiert die Portnummer des Anwendungsservers.

2. Klicken Sie auf "Directories" (Verzeichnisse).

   Das CA IdentityMinder-Verzeichnisfenster wird geöffnet.

3. Klicken Sie auf "Create from Wizard" (Über Assistenten erstellen).

4. Geben Sie den Pfad und Dateinamen der Verzeichnis-XML-Datei für das Konfigurieren des Bereitstellungsverzeichnisses ein. Es wird unter "directoryTemplates\ProvisioningServer" im Ordner "Verwaltung" gespeichert. Der Standardspeicherort dieses Ordners ist:

   - Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   **Hinweis:** Sie können diese Verzeichniskonfigurationsdatei wie installiert ohne Änderungen verwenden.

5. Klicken Sie auf "Weiter".

6. Geben Sie Werte für die Felder in diesem Fenster folgendermaßen an:

   **Name**

   Ist ein Name für das Bereitstellungsverzeichnis, das dem Bereitstellungsserver zugeordnet wird, den Sie konfigurieren.

   - Wenn CA IdentityMinder nicht in SiteMinder integriert ist, geben Sie einen aussagekräftigen Namen für das Objekt an, das CA IdentityMinder verwendet, um mit dem Benutzerverzeichnis Verbindung aufzunehmen.
   - Wenn CA IdentityMinder in SiteMinder integriert ist, haben Sie zwei Optionen:

     Wenn Sie ein Benutzerverzeichnis-Verbindungsobjekt in SiteMinder erstellen wollen, geben Sie einen aussagekräftigen Namen an. CA IdentityMinder erstellt dieses Objekt in SiteMinder mit dem Namen, den Sie angeben.

     Wenn Sie mit einem vorhandenen SiteMinder-Benutzerverzeichnis Verbindung aufnehmen wollen, geben Sie den Namen des SiteMinder-Benutzerverzeichnis-Verbindungsobjekts genau an, wie er in der Richtlinienserver-Benutzeroberfläche angezeigt wird.

   **Beschreibung**

   (Optional) Beschreibt das CA IdentityMinder-Verzeichnis.

   **Host**

   Gibt den Hostnamen oder die IP-Adresse des Servers an, auf dem das Benutzerverzeichnis installiert ist.

   **Port**

   Gibt die Portnummer des Benutzerverzeichnisses an.

**Domäne**

Gibt den Namen der Bereitstellungsdomäne an, die CA IdentityMinder verwaltet.

**Wichtig!** Wenn Sie ein Bereitstellungsverzeichnis über die Management-Konsole mit fremdsprachigen Zeichen als Domänenname erstellen, schlägt die Bereitstellungsverzeichnis-Erstellung fehl.

Der Name muss mit dem Namen der Bereitstellungsdomäne übereinstimmen, den Sie während Installation angaben.

**Hinweis:** Der Domänenname berücksichtigt Groß- und Kleinschreibung.

**Benutzername**

Gibt einen Benutzer an, der sich beim Bereitstellungsmanager anmelden kann.

Der Benutzer muss das Domänenadministrator-Profil oder ein gleichwertiges Set von Berechtigungen für die Bereitstellungsdomäne haben.

**Kennwort**

Gibt das Kennwort für den globalen Benutzer an, den Sie im Feld "Benutzername" angegeben haben.

**Kennwort bestätigen**

Geben Sie das in das Feld "Kennwort" eingegebene Kennwort erneut zur Bestätigung ein.

**Sichere Verbindung**

Zeigt an, ob CA IdentityMinder eine sichere Verbindung verwendet.

Wählen Sie diese Option für Active Directory-Benutzerspeicher aus.

**Verzeichnissuchparameter**

**maxrows** definiert die Höchstanzahl von Ergebnissen, die CA IdentityMinder zurückgeben kann, wenn man ein Benutzerverzeichnis durchsucht. Dieser Wert überschreibt ein im LDAP-Verzeichnis festgelegtes Limit. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Hinweis:** Der maxrows-Parameter beschränkt nicht die Anzahl von Ergebnissen, die im CA IdentityMinder-Aufgabenfenster angezeigt werden. Um die Anzeigeeinstellungen zu konfigurieren, ändern Sie die Listenfensterdefinition in der CA IdentityMinder-Benutzerkonsole. Weitere Anweisungen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**timeout** bestimmt die maximale Anzahl von Sekunden, die CA IdentityMinder ein Verzeichnis durchsucht, bevor es die Suche beendet.

**Failover-Verbindungen**

Hostname und Portnummer von einem oder mehreren optionalen Systemen, die alternative Bereitstellungsserver sind. Wenn mehrere Server aufgelistet sind, versucht CA IdentityMinder, mit den Systemen in der Reihenfolge Verbindung aufzunehmen, in der sie aufgelistet sind.

Die alternativen Bereitstellungsserver werden verwendet, wenn der primäre Bereitstellungsserver fehlschlägt. Wenn der primäre Bereitstellungsserver erneut verfügbar wird, wird der alternative Bereitstellungsserver weiterhin verwendet. Wenn Sie zur Verwendung des Bereitstellungsservers zurückkehren möchten, starten Sie den alternativen Bereitstellungsserver neu.

7. Klicken Sie auf "Weiter".
8. Wählen Sie die zu verwaltenden Objekte aus, wie Benutzer oder Gruppen.
9. Nachdem Sie die Objekte nach Bedarf konfiguriert haben, lassen Sie die Zusammenfassung der Bereitstellung des Verzeichnisses anzeigen und überprüfen die Einstellungen für das Bereitstellungsverzeichnis.
10. Klicken Sie auf eine dieser Aktionen:
    a. Klicken Sie auf "Zurück", um etwas zu ändern.
    b. Klicken Sie auf "Speichern", um die Verzeichnisinformationen zu speichern, wenn Sie später zur Bereitstellung zurückkommen wollen.
    c. Klicken Sie auf "Fertig stellen", um diesen Vorgang abzuschließen und anzufangen, eine Umgebung für die Bereitstellung zu konfigurieren (siehe Seite 199).

# Anzeigen von CA IdentityMinder-Verzeichnissen

Führen Sie den folgenden Vorgang aus, um ein CA IdentityMinder-Verzeichnis anzuzeigen.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der CA IdentityMinder-Management-Konsole auf "Directories" (Verzeichnisse).
2. Klicken Sie auf den Namen des anzuzeigenden CA IdentityMinder-Verzeichnisses. Das Fenster //"Verzeichniseigenschaften" wird mit den CA IdentityMinder-Verzeichniseigenschaften angezeigt.

# CA IdentityMinder-Verzeichniseigenschaften

Die CA IdentityMinder-Verzeichniseigenschaften sind wie folgt:

**Hinweis**: Die Eigenschaften, die angezeigt werden, hängen vom Typ der Datenbank oder des Verzeichnisses ab, das dem CA IdentityMinder-Verzeichnis zugeordnet ist.

**Name**

Definiert den eindeutigen Namen des CA IdentityMinder-Verzeichnisses.

**Beschreibung**

Geben Sie eine Beschreibung des CA IdentityMinder-Verzeichnisses ein.

**Typ**

Definiert den Typ des Verzeichnisanbieters.

**Connection Object Name (Name des Verbindungsobjekts)**

Zeigt den Namen des Benutzerverzeichnisses an, das das CA IdentityMinder-Verzeichnis beschreibt.

Wenn CA IdentityMinder in SiteMinder integriert ist, stimmt der Verbindungsobjektname mit dem Namen der SiteMinder-Benutzerverzeichnisverbindung überein.

**Root Organization (Stammorganisation), für Benutzerspeicher, die Organisationen einschließen**

Gibt den Eingangspunkt für den Benutzerspeicher an.

Für LDAP-Verzeichnisse wird die Stammorganisation als DN angegeben. Für relationale Datenbanken wird die eindeutige Kennung für die Stammorganisation angezeigt.

**JDBC Data Source (JDBC-Datenquelle)**

Gibt den Namen der JDBC-Datenquelle an, die CA IdentityMinder verwendet, um mit der Datenbank Verbindung aufzunehmen.

**URL**

Gibt die URL oder IP-Adresse des Benutzerspeichers an.

**Benutzername**

Gibt den Benutzernamen für ein Konto an, das auf den Benutzerspeicher zugreifen kann.

**Search Maximum Rows (Maximale Such-Zeilen)**

Zeigt die Höchstanzahl von zurückgegebenen Zeilen als Ergebnis einer Suche an.

**Search Page Size (Suchseiten-Größe)**

Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

**Hinweis:** Der Benutzerspeicher, den CA IdentityMinder verwaltet, muss Paging unterstützen. Einige Benutzerspeichertypen können zusätzliche Konfiguration erfordern, um Paging zu unterstützen. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

**Supports Paging (Unterstützt Paging)**

Zeigt an, dass das Verzeichnis Paging unterstützt.

**Search Timeout (Such-Zeitlimit), nur für LDAP-Verzeichnisse**

Gibt die maximale Anzahl von Sekunden, die CA IdentityMinder einen Benutzerspeicher durchsucht, bevor es die Suche beendet.

**Provisioning Domain (Bereitstellungsdomäne), nur für Bereitstellungsserververzeichnisse**

Bereitstellungsdomäne, die CA IdentityMinder verwaltet.

## Fenster "CA IdentityMinder Directory Properties" (Verzeichniseigenschaften)

Im Eigenschaftsfenster werden allgemeine Informationen über das von Ihnen ausgewählte CA IdentityMinder-Verzeichnis angezeigt. Das Fenster "Directory Properties" ist in die folgenden Abschnitte auf geteilt:

**Directory Properties**

Zeigt grundlegende Eigenschaften für das CA IdentityMinder-Verzeichnis einschließlich der zugeordneten Bereitstellungsdomäne an, wenn Bereitstellung für die Umgebung aktiviert ist.

**Managed Objects (Verwaltete Objekte)** **(siehe Seite 181)**

Gibt Beschreibungen des Typs von Benutzerspeicherobjekten an, die CA IdentityMinder verwaltet.

**Validation Rule Sets (Validierungsregelsätze)** **(siehe Seite 185)**

Listet Validierungsregelsätze auf, die sich auf das CA IdentityMinder-Verzeichnis beziehen.

**Environments (Umgebungen)**

Listet die Umgebungen auf, die dem CA IdentityMinder-Verzeichnis zugeordnet werden. Ein Verzeichnis kann mehreren CA IdentityMinder-Umgebungen zugeordnet werden.

Um weitere Informationen zu einer CA IdentityMinder-Umgebung anzuzeigen, klicken Sie auf den Namen der Umgebung.

Um Eigenschaften in einem CA IdentityMinder-Verzeichnis zu ändern, importieren Sie eine Verzeichniskonfigurationsdatei, wie in Aktualisieren von CA IdentityMinder-Verzeichnissen (siehe Seite 188) beschrieben.

Zusätzlich zum Anzeigen der Eigenschaften können Sie auch die folgenden Aktionen ausführen:

**Update Authentication (Authentifizierung aktualisieren)**

Erlaubt Administratoren, das Verzeichnis zu ändern, das CA IdentityMinder verwendet, um Management-Konsolen-Administratoren zu authentifizieren. Administratoren können auch zusätzliche Management-Konsolen-Administratoren im vorhandenen Authentifizierungsverzeichnis hinzufügen.

**Hinweis:** Die Optionen zum Aktualisieren der Authentifizierung gelten nur, wenn systemeigene CA IdentityMinder-Sicherheit die Management-Konsole schützt. Information zum Aktivieren der systemeigenen Sicherheit oder zur Verwendung einer anderen Sicherheitsmethode finden Sie im *Konfigurationshandbuch*.

**Export** **(siehe Seite 187)**

Exportiert die Verzeichnisdefinition als XML-Datei. Nachdem Sie die Verzeichniseinstellungen exportiert haben, können Sie die XML-Datei ändern und dann erneut importieren, um das Verzeichnis zu aktualisieren. Sie können auch die XML-Datei in ein anderes Verzeichnis importieren, um die gleichen Einstellungen für dieses Verzeichnis zu konfigurieren.

**Aktualisieren** **(siehe Seite 188)**

Ermöglicht Administratoren das Hinzufügen oder Ändern von verwalteten Objektdefinitionen, wie die Attribute eines Objekts, Festlegen von Suchparametern und Ändern von Verzeichniseigenschaften.

# Anzeigen von verwalteten Objekteigenschaften und Attributen

Ein verwaltetes Objekt beschreibt einen Eintragstyp im Benutzerspeicher, wie ein Benutzer, Gruppe oder Organisation. Die Eigenschaften und Attribute, die sich auf ein verwaltetes Objekt beziehen, beziehen sich auf alle Einträge dieses Typs. Zum Beispiel besteht ein Benutzerprofil aus allen Eigenschaften und Attributen des verwalteten Objekts "Benutzer".

Um die Details eines verwalteten Objekts anzuzeigen, klicken Sie auf den Namen des Objekts, um das Fenster "Managed Object Properties" (Eigenschaften von verwalteten Objekten) zu öffnen.

## Managed Object Properties (Eigenschaften von verwalteten Objekten)

Das Fenster "Managed Object Properties" beschreibt die Eigenschaften und Attribute für einen Typ von verwaltetem Objekt.

Die Informationen im Fenster "Managed Object Properties" hängen vom Typ des Benutzerspeichers ab, den Sie verwalten. Verwaltete Eigenschaften eines Objekts sind Folgende:

**Beschreibung**

Gibt eine Beschreibung des verwalteten Objekts an.

**Typ**

Zeigt den Eintragstyp an, den das verwaltete Objekt darstellt. Ein Objekttyp kann einer der folgenden Typen sein:

- User
- Gruppe
- Organisation

**Objektklasse (nur für LDAP-Verzeichnisse)**

Gibt die Objektklassen für das verwaltete Objekt an. Ein verwaltetes Objekt kann mehrere Objektklassen haben.

**Sort Order (Sortierreihenfolge), nur für LDAP-Verzeichnisse**

Gibt die Attribute an, die CA IdentityMinder verwendet, um Suchergebnisse nach benutzerdefinierter Business-Logik zu sortieren. Die Reihenfolge wirkt sich nicht auf die Reihenfolge von Suchergebnissen in der Benutzerkonsole aus.

Wenn Sie zum Beispiel das cn-Attribut für das Benutzerobjekt angeben, sortiert CA IdentityMinder die Ergebnisse einer Suche nach Benutzern alphabetisch nach dem cn-Attribut.

**Primary Table (Primäre Tabelle), nur für relationale Datenbanken**

Gibt die Tabelle an, die die eindeutige Kennung für das verwaltete Objekt enthält.

**Maximale Zeilenzahl**

Gibt die Höchstanzahl von Ergebnissen an, die CA IdentityMinder zurückgeben kann, wenn man nach Objekten dieses Typs sucht. Wenn die Anzahl von Ergebnissen das Limit überschreitet, wird ein Fehler angezeigt.

Das Einstellen der maximalen Zeilenanzahl kann die Einstellungen im LDAP-Verzeichnis überschreiben, die Suchergebnisse beschränken. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Seitengröße**

Gibt die Anzahl von Objekten an, die in einer einzelnen Suche zurückgegeben werden können. Wenn die Anzahl von Objekten die Seitengröße überschreitet, führt CA IdentityMinder mehrere Suchen aus.

**Hinweis:** Der Benutzerspeicher, den CA IdentityMinder verwaltet, muss Paging unterstützen. Einige Benutzerspeichertypen können zusätzliche Konfiguration erfordern, um Paging zu unterstützen. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

## Container-Eigenschaften (nur für LDAP-Verzeichnisse)

In einem LDAP-Verzeichnis enthält die *Container*-Gruppe Objekte von einem bestimmten Typ. Wenn ein Container angegeben wird, verarbeitet CA IdentityMinder nur Einträge im Container. Wenn Sie zum Beispiel den Container "ou=People" angeben, verarbeitet CA IdentityMinder nur Benutzer, die im People-Container vorhanden sind.

**Hinweis:** Benutzer und Gruppen, die im LDAP-Verzeichnis, aber nicht im definierten Container vorhanden sind, können in der Benutzerkonsole angezeigt werden. Es kann jedoch Probleme geben, wenn man diese Benutzer und Gruppen verwaltet.

Container gruppieren nur Benutzer und Gruppen. Sie können keinen Container für Organisationen angeben.

Zu den Eigenschaften eines Containers gehören:

**objectclass**

Gibt die LDAP-Objektklasse des Containers an, wo Objekte von einem bestimmten Typ erstellt werden. Zum Beispiel ist der Standardwert für den Benutzercontainer "top,organizationalUnit", was anzeigt, dass Benutzer in LDAP-Organisationseinheiten (ou) erstellt werden.

**ID**

Gibt das Attribut an, das den Containernamen, zum Beispiel "ou", speichert. Das Attribut wird mit dem Namenswert paarweise angeordnet, um den zugehörigen DN des Containers zu bilden, wie im folgenden Beispiel:

ou=People

**Name**

Gibt den Namen des Containers an.

## Eigenschaften von sekundären Tabellen (nur für relationale Datenbanken)

Sekundäre Tabellen enthalten zusätzliche Attribute für ein verwaltetes Objekt. Zum Beispiel kann eine sekundäre Tabelle namens "tblUserAddress" die Attribute für Straße, Stadt, Land und Postleitzahl für das verwaltete Objekt "Benutzer" enthalten.

Die folgenden Eigenschaften werden für sekundäre Tabellen angezeigt:

**Tabelle**

Gibt den Namen der Tabelle an.

**Referenz**

Beschreibt die Zuordnung zwischen der primären Tabelle und der sekundären Tabelle.

Die Referenz wird mithilfe des folgenden Formats angezeigt:

*primarytable.attribute=secondarytable.attribute*

Zum Beispiel zeigt "tblUsers.id = tblUserAddress.userid" an, dass das id-Attribut in der primären Tabelle "tblUsers" zum userid-Attribut in der Tabelle "tblUserAddress" zugeordnet wird.

## Attributeigenschaften im Fenster "Managed Object Properties"

Die folgenden Eigenschaften werden für Attribute im Fenster "Managed Object Properties" (Eigenschaften von verwalteten Objekten) angezeigt:

**Anzeigename**

Der benutzerfreundliche Name des Attributs. Dieser Name wird in der Liste der verfügbaren Attribute angezeigt, wenn Sie ein Aufgabenfenster für eine bestimmte Aufgabe in der Benutzerkonsole entwerfen.

**Physischer Name**

Der Name des Attributs im Benutzerspeicher.

**Benutzername "Well-Known"**

Der bekannte Benutzername "Well-Known" zeigt Attribute an, die eine besondere Bedeutung in CA IdentityMinder haben, wie das Attribut, das verwendet wird, um Benutzerkennwörter zu speichern.

## Attributeigenschaften in den Attributeigenschaften-Fenstern

Sie können zusätzliche Details über ein Attribut anzeigen, indem Sie auf seinen Namen klicken, um das Attributeigenschaften-Fenster zu öffnen.

Die folgenden Attributeigenschaften werden im Fenster "Attribute Properties" (Attributeigenschaften) angezeigt:

**Beschreibung**

Geben Sie eine Beschreibung des Attributs ein.

**Physischer Name**

Gibt den Namen des Attributs im Benutzerspeicher an.

**Objektklasse (nur für Benutzer-, Gruppen- und Organisationsattribute in LDAP-Verzeichnissen)**

Die zusätzliche LDAP-Klasse für ein Benutzerattribut, wenn das Attribut nicht Teil der primären Objektklasse ist, die für das Benutzerobjekt angegeben ist.

Sie können nur für Benutzer- und Gruppenobjekte eine zusätzliche Objektklasse angeben.

**Benutzername "Well-Known"**

Zeigt Attribute an, die eine besondere Bedeutung in CA IdentityMinder haben, wie das Attribut, das verwendet wird, um Benutzerkennwörter zu speichern.

**erforderlich**

Zeigt an, ob ein Wert für das Attribut erforderlich ist, wie folgt:

- "True" gibt an, dass das Attribut einen Wert haben muss.
- "False" gibt an, dass ein Wert optional ist.

**Schreibgeschützt**

Zeigt die Berechtigungsebene für ein Attribut an, wie folgt:

- "True" gibt an, dass das Attribut nicht geändert werden kann.
- "False" gibt an, dass das Attribut geändert werden kann.

**Ausgeblendet**

Zeigt an, ob ein Attribut in einem Aufgabenfenster für eine bestimmte Aufgabe angezeigt werden kann.

Ausgeblendete Attribute werden oft in logischen Attributschemen verwendet.

**Hinweis:** Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

**Unterstützt mehrere Werte**

Zeigt an, ob das Attribut mehrere Werte haben kann oder nicht, wie folgt (zum Beispiel hat das Attribut, das verwendet wird, um die Mitglieder von einer Gruppe zu speichern, mehrere Werte):

- "True" gibt an, dass das Attribut mehrere Werte unterstützen kann.
- "False" gibt an, dass das Attribut nur einen einzelnen Wert haben kann.

**Multiple Value Delimiter (Trennzeichen bei mehreren Werten), nur für relationale Datenbanken**

Das Zeichen, das Werte voneinander trennt, wenn mehrere Werte in einer Spalte gespeichert werden.

**System Attribute (Systemattribut)**

Zeigt an, ob das Attribut nur von CA IdentityMinder verwendet wird, wie folgt:

- "True" zeigt an, dass das Attribut ein Systemattribut ist. Das Attribut ist nicht zum Hinzufügen zu Aufgabenfenstern verfügbar.
- "False" zeigt an, dass die Benutzer dieses Attribut verwenden können. Das Attribut kann in Aufgabenfenstern angezeigt werden.

**Datentyp**

Gibt den Datentyp des Attributs an. Der Standardwert ist "String".

**Maximum Length (Maximale Länge)**

Gibt die größtmögliche Länge an, die ein Attributwert haben kann. Wenn auf 0 festgelegt, gibt es kein Limit für die Länge des Wertes.

**Validation Rule Set (Validierungsregelsatz)**

Gibt den Namen eines Validierungsregelsatzes an, falls das Attribut einem zugeordnet ist.

## Validation Rule Sets (Validierungsregelsätze)

Eine Validierungsregel erzwingt Anforderungen für Daten, die ein Benutzer in ein Aufgabenfensterfeld eingibt. Die Anforderungen können einen Datentyp oder ein Format erzwingen oder können sicherstellen, dass die Daten im Kontext von anderen Daten im Aufgabenfenster gültig sind.

Eine oder mehrere Validierungsregeln werden in einem Validierungsregelsatz gruppiert. Ein Validierungsregelsatz wird dann einem Profilattribut zugeordnet. Zum Beispiel können Sie einen Validierungsregelsatz erstellen, der eine Format/Datum-Validierungsregel enthält, die ein Datumsformat von mm-tt-jjjj erzwingt. Sie können dann den Validierungsregelsatz dem Attribut zuordnen, das das Startdatum eines Mitarbeiters speichert.

**Hinweis:** Sie erstellen Validierungsregeln und Regelsätze in der Verzeichniskonfigurationsdatei oder in der Benutzerkonsole.

Das Fenster "Managed Object Properties" (Eigenschaften von verwalteten Objekten) zeigt eine Liste von Validierungsregelsätzen an, die sich auf das CA IdentityMinder-Verzeichnis beziehen. Um die Details eines Validierungsregelsatzes anzuzeigen, klicken Sie auf den Namen des Regelsatzes, um das Fenster "Validation Rule Set Properties" (Validierungsregelsatz-Eigenschaften) zu öffnen.

## Validierungsregel-Eigenschaften

Die folgenden Informationen werden im Fenster "Validation Rule Properties" (Validierungsregel-Eigenschaften) angezeigt:

**Name**

Gibt den Namen der Validierungsregel an.

**Beschreibung**

Gibt eine Beschreibung der Regel an.

**Klasse**

Gibt den Namen der Java-Klasse an, die die Validierungsregel implementiert.

Dieses Feld wird nicht angezeigt, außer wenn die Validierungsregel in einer Java-Klasse definiert ist.

**Dateiname**

Gibt den Namen der Datei an, die die JavaScript-Implementierung der Validierungsregel enthält.

Dieses Feld wird nicht angezeigt, außer wenn die Validierungsregel in einer Datei definiert ist.

**Regulärer Ausdruck**

Gibt den regulären Ausdruck an, der die Validierungsregel implementiert.

Dieses Feld wird nicht angezeigt, außer wenn die Validierungsregel als regulärer Ausdruck definiert ist.

## Validierungsregelsatz-Eigenschaften

Die folgenden Informationen werden im Fenster "Validation Rule Set Properties" (Validierungsregelsatz-Eigenschaften) angezeigt:

**Name**

Gibt den Namen des Validierungsregelsatzes an.

**Beschreibung**

Gibt eine Beschreibung für den Validierungsregelsatz an.

Die Validierungsregelsatz-Eigenschaftsseite schließt auch eine Liste von Validierungsregeln im Set ein. Sie können auf den Namen der Validierungsregel klicken, um das Fenster "Validation Rule Properties" (Validierungsregel-Eigenschaften) zu öffnen.

# Aktualisieren von Einstellungen für ein CA IdentityMinder-Verzeichnis

Um die aktuellen Einstellungen von einem CA IdentityMinder-Verzeichnis anzuzeigen, exportieren Sie die Verzeichniseinstellungen und speichern sie als eine XML-Datei.

Nachdem Sie die Verzeichniseinstellungen exportiert haben, können Sie die XML-Datei ändern und erneut importieren, um das Verzeichnis zu aktualisieren. Sie können auch die XML-Datei in ein anderes Verzeichnis importieren, um die gleichen Einstellungen für dieses Verzeichnis zu konfigurieren.

## Exportieren von CA IdentityMinder-Verzeichnissen

Führen Sie den folgenden Vorgang aus, um ein CA IdentityMinder-Verzeichnis zu exportieren.

**Gehen Sie wie folgt vor:**

1. Klicken Sie auf "Directories" (Verzeichnisse).

   Die Liste von CA IdentityMinder-Verzeichnissen wird angezeigt.

2. Klicken Sie auf den Namen des zu exportierenden Verzeichnisses.

   Die Eigenschaften für das CA IdentityMinder-Verzeichnisfenster werden angezeigt.

3. Klicken Sie unten im Eigenschaftsfenster auf "Export".
4. Wenn Sie aufgefordert werden, speichern Sie die XML-Datei.

## Aktualisieren von CA IdentityMinder-Verzeichnissen

Der Zweck der Aktualisierung eines CA IdentityMinder-Verzeichnisses ist:

- Hinzufügen oder Ändern von verwalteten Objektdefinitionen, einschließlich der Attribute eines Objekts.
- Festlegen von Suchparametern
- Ändern der Verzeichniseigenschaften

**Hinweis:** CA IdentityMinder löscht keine Objekt- oder Attributdefinitionen.

Die Verzeichniskonfigurationsdatei darf nur die Änderungen enthalten, die Sie vornehmen wollen. Sie sollten keine Eigenschaften oder Attribute einschließen, die bereits definiert sind.

**Hinweis:** Wenn Sie einen Cluster von CA IdentityMinder-Knoten haben, kann nur ein CA IdentityMinder-Knoten aktiviert sein, wenn Sie Änderungen in der Management-Konsole vornehmen. Halten Sie alle außer einen CA IdentityMinder-Knoten an, bevor Sie ein CA IdentityMinder-Verzeichnis erstellen oder ändern.

**Gehen Sie wie folgt vor:**

1. Exportieren Sie die aktuellen CA IdentityMinder-Verzeichniseinstellungen in eine XML-Datei.
2. Ändern Sie die XML-Datei, um Ihre Änderungen widerzuspiegeln.
3. Klicken Sie auf "Directories" (Verzeichnisse).

   Die Liste von CA IdentityMinder-Verzeichnissen wird angezeigt.
4. Klicken Sie auf den Namen des zu aktualisierenden Verzeichnisses.

   Die Eigenschaften für das CA IdentityMinder-Verzeichnis werden angezeigt.
5. Klicken unten im Eigenschaftsfenster auf "Aktualisieren".
6. Geben Sie den Pfad und Dateinamen der XML-Datei für das Aktualisieren des CA IdentityMinder-Verzeichnisses ein, oder suchen Sie nach der Datei. Klicken Sie auf "Fertig stellen".

   Statusinformationen werden im Verzeichniskonfigurations-Ausgabefeld angezeigt.
7. Klicken Sie auf "Fortfahren".

## Löschen von CA IdentityMinder-Verzeichnissen

Bevor Sie ein CA IdentityMinder-Verzeichnis löschen, löschen Sie CA IdentityMinder-Umgebungen, die ihm zugeordnet sind.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Directories" (Verzeichnisse).

   Die Liste von CA IdentityMinder-Verzeichnissen wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen links von dem zu löschenden Verzeichnis (oder den Verzeichnissen).
3. Klicken Sie auf "Löschen".

   Eine Bestätigungsmeldung wird angezeigt.

4. Klicken Sie auf "OK", um den Löschvorgang zu bestätigen.

# Kapitel 6: CA IdentityMinder-Umgebungen

Dieses Kapitel enthält folgende Themen:

CA IdentityMinder-Umgebungen (siehe Seite 191)
Voraussetzungen für das Erstellen von CA IdentityMinder-Umgebungen (siehe Seite 192)
Erstellen einer CA IdentityMinder-Umgebung (siehe Seite 193)
Zugreifen auf eine CA IdentityMinder-Umgebung (siehe Seite 198)
Konfigurieren einer Umgebung für die Bereitstellung (siehe Seite 199)
Verwalten von Umgebungen (siehe Seite 212)
Verwalten von Konfigurationen (siehe Seite 220)
Optimieren der Auswertung von Richtlinienregeln (siehe Seite 227)
Role and Task Settings (Rollen- und Aufgabeneinstellungen) (siehe Seite 228)
Ändern des Systemmanager-Kontos (siehe Seite 230)
Aufrufen des Status einer CA IdentityMinder-Umgebung (siehe Seite 232)

## CA IdentityMinder-Umgebungen

Eine CA IdentityMinder-Umgebung ist eine Ansicht eines Benutzerspeichers. In einer CA IdentityMinder-Umgebung können Sie Benutzer, Gruppen, Organisationen, Aufgaben und Rollen verwalten. Außerdem können Sie den Benutzern Konten in verwalteten Endpunkten, zum Beispiel E-Mail-Konten oder andere Anwendungen, zur Verfügung stellen.

Mithilfe der Management-Konsole können Sie die folgenden Aufgaben ausführen:

- Erstellen, Ändern oder Löschen einer CA IdentityMinder-Umgebung
- Exportieren und Importieren einer CA IdentityMinder-Umgebung
- Konfigurieren der erweiterten Einstellungen
- Importieren von Rollen und Aufgaben
- Zurücksetzen des Systemmanager-Kontos

# Voraussetzungen für das Erstellen von CA IdentityMinder-Umgebungen

Bevor Sie anfangen, verwenden Sie das Arbeitsblatt in der folgenden Tabelle, um die erforderlichen Informationen zu erfassen:

| **Arbeitsblatt für die Konfiguration einer CA IdentityMinder-Umgebung** | |
|---|---|
| **Erforderliche Informationen** | **Wert** |
| Ein von Ihnen gewählter, aussagekräftiger CA IdentityMinder-Umgebungsname.<br>Beispiel: MeineUmgebung | |
| Eine Basis-URL, die CA IdentityMinder verwendet, um eine Umleitungs-URL für die Standardkennwortrichtlinie für die Umgebung zu bilden.<br>Beispiel:<br>http://server.yourcompany.org | |
| Ein Alias, der der URL für den Zugriff auf geschützte Aufgaben in der Umgebung hinzugefügt wird.<br>Beispiel:<br>http://server.yourcompany.org/iam/im/alias | |
| Ein Alias, der der URL für den Zugriff auf öffentliche Aufgaben, zum Beispiel Selbstregistrierungsaufgaben und Aufgaben in Bezug auf vergessene Kennwörter, hinzugefügt wird.<br>Beispiel:<br>http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration<br>**Hinweis:** Wenn Ihre Umgebung keine öffentlichen Aufgaben einschließt, ist es nicht erforderlich, einen öffentlichen Alias anzugeben. | |
| Wenn Sie einen öffentlichen Alias angegeben haben, der Name eines vorhandenen Benutzers, der als öffentlicher Benutzer fungiert. CA IdentityMinder verwendet beim Zugriff auf öffentliche Aufgaben anstelle der Anmeldeinformationen des Benutzers die Anmeldeinformationen des öffentlichen Benutzers. | |
| Name von CA IdentityMinder (siehe Seite 103) | |

| **Arbeitsblatt für die Konfiguration einer CA IdentityMinder-Umgebung** | |
|---|---|
| **Erforderliche Informationen** | **Wert** |
| Der Name des Bereitstellungsverzeichnisses, wenn die CA IdentityMinder-Umgebung die Bereitstellung unterstützt. | |
| Die eindeutige Kennung für einen vorhandenen Benutzer, der die CA IdentityMinder-Umgebung verwaltet.<br>Zum Beispiel: MeinAdmin | |
| Der Name des SiteMinder-Agenten oder der Agentengruppe, der bzw. die die CA IdentityMinder-Umgebung schützt, wenn CA IdentityMinder mit SiteMinder integriert wird. | |

# Erstellen einer CA IdentityMinder-Umgebung

Über CA IdentityMinder-Umgebungen können Sie Objekte in einem Verzeichnis mit einem Rollen- und Aufgabensatz verwalten. Verwenden Sie den CA IdentityMinder-Umgebungs-Assistenten, der Sie schrittweise durch die Erstellung einer CA IdentityMinder-Umgebung leitet.

Beachten Sie vor der Erstellung einer CA IdentityMinder-Umgebung Folgendes:

- Gehen Sie davon aus, dass Sie einen LDAP-Benutzerspeicher verwenden und einen Benutzercontainer wie ou=People in der Verzeichniskonfigurationsdatei (directory.xml) für Ihr CA IdentityMinder-Verzeichnis konfiguriert haben. Vergewissern Sie sich, dass die Benutzer, die Sie auswählen, wenn Sie die CA IdentityMinder-Umgebung erstellen, in diesem Container vorhanden sind. Die Auswahl eines Benutzerkontos, das im Benutzercontainer nicht vorhanden ist, kann Fehler verursachen.
- Wenn Sie eine CA IdentityMinder-Umgebung konfigurieren, um ein LDAP-Benutzerverzeichnis mit einer flachen Benutzerstruktur zu verwalten, muss das Profil für den ausgewählten Benutzer die Organisation des Benutzers einschließen. Um sicherzustellen, dass das Profil eines Benutzers richtig konfiguriert wird, fügen Sie dem physischen Attribut, das dem bekannten Attribut %ORG_MEMBERSHIP% in der directory.xml-Datei (siehe Seite 87) entspricht, den Namen der Organisation des Benutzers hinzu. Wenn zum Beispiel die Beschreibung des physischen Attributs dem bekannten Attribut %ORG_MEMBERSHIP% in der directory.xml-Datei zugeordnet ist und der Benutzer zur Organisation "Employees" gehört, muss das Profil des Benutzers das Attribut-/Wertpaar "description=Employees" enthalten.

**Gehen Sie wie folgt vor:**

1. Wenn CA IdentityMinder einen Richtlinienserver-Cluster verwendet, beenden Sie alle bis auf einen Richtlinienserver.
2. Wenn Sie einen Cluster von CA IdentityMinder-Knoten haben, beenden Sie alle bis auf einen CA IdentityMinder-Knoten.
3. Klicken Sie in der Managementkonsole auf "Umgebungen".
4. Klicken Sie auf "Neu".

   Der CA IdentityMinder-Umgebungs-Assistent wird geöffnet.
5. Geben Sie die folgenden Informationen an:

   ■ **Umgebungs-Name**

   Gibt einen eindeutigen Namen für die Umgebung an.

   ■ **Beschreibung**

   Beschreibt die Umgebung.

   ■ **Protected Alias (Geschützter Alias)**

   Gibt einen eindeutigen Namen, zum Beispiel Mitarbeiter, an. Dieser Alias wird der URL für den Zugriff auf geschützte Aufgaben in der CA IdentityMinder-Umgebung hinzugefügt. Wenn dieser Alias zum Beispiel "employees" ist, lautet die URL für den Zugriff auf die Mitarbeiterumgebung http://my*server.mycompany.com*/iam/im/employees.

   **Hinweis:** Für den Alias wird die Groß-/Kleinschreibung berücksichtigt, und er darf keine Leerzeichen enthalten. Es wird empfohlen, für den Alias Kleinbuchstaben und keine Satzzeichen oder Leerzeichen zu verwenden.

   ■ **Base URL (Basis-DN)**

   Gibt die URL für CA IdentityMinder an. Die URL erfordert einen Hostnamen; "localhost" ist nicht zulässig. Schließen Sie auch nicht den Alias ein, zum Beispiel http://*myserver.mycompany.com*/iam/im.

   Wenn Sie einen Web-Agenten verwenden, vergewissern Sie sich, dass die Basis-URL geändert wurde und die URL des Web-Agenten widerspiegelt.

   **Hinweis**: Wenn Sie einen Web-Agenten verwenden, um CA IdentityMinder-Ressourcen zu schützen, geben Sie im Feld "Basis-URL" keine Portnummer an. Wenn Sie einen Web-Agenten verwenden und die Basis-URL eine Portnummer enthält, funktionieren die Links zu CA IdentityMinder-Aufgaben nicht ordnungsgemäß.

   Weitere Informationen zum Schutz von CA IdentityMinder-Ressourcen finden Sie im *Installationshandbuch* für Ihren Anwendungsserver.

   Klicken Sie auf "Weiter".
6. Wählen Sie ein CA IdentityMinder-Verzeichnis aus, um es der Umgebung zuzuordnen, die Sie erstellen, und klicken Sie auf "Weiter".

7. Wenn die CA IdentityMinder-Umgebung die Bereitstellung unterstützt, wählen Sie den entsprechenden Bereitstellungsserver für die Verwendung aus.

   **Hinweis:** Sie werden nicht aufgefordert, einen Bereitstellungsserver auszuwählen, wenn Sie ein Bereitstellungsverzeichnis als CA IdentityMinder-Verzeichnis ausgewählt haben.

8. Konfigurieren Sie die Unterstützung von öffentlichen Aufgaben. Diese Aufgaben sind in der Regel Self-Service-Aufgaben wie Selbstregistrierungsaufgaben und Aufgaben in Bezug auf vergessene Kennwörter. Benutzer müssen sich nicht anmelden, um auf öffentliche Aufgaben zuzugreifen.

   **Hinweis:** Damit Benutzer Self-Service-Aufgaben verwenden können, konfigurieren Sie die Unterstützung von öffentlichen Aufgaben.

   a. Geben Sie einen eindeutigen Namen an, der zur URL für den Zugriff auf öffentliche Aufgaben hinzugefügt wird.

      **Beispiel:** Mithilfe der folgenden URL können Sie auf die standardmäßige Selbstregistrierungsaufgabe zugreifen:

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistra tion

      In dieser URL ist *alias* der eindeutige Name, den Sie angeben.

   b. Geben Sie eins der folgenden vorhandenen Benutzerkonten an, das als öffentliches Benutzerkonto dient. CA IdentityMinder ermöglicht mit diesem Konto unbekannten Benutzern den Zugriff auf öffentliche Aufgaben ohne die Angabe von Anmeldeinformationen.

      − LDAP-Benutzer geben die eindeutige Kennung oder den zugehörigen DN des öffentlichen Benutzerkontos ein. Vergewissern Sie sich, dass dieser Wert dem bekannten Attribut %USER_ID% (siehe Seite 79) zugeordnet ist. Wenn der DN des Benutzer-DN zum Beispiel uid=Admin1, ou=People, ou=Employees, ou=NeteAuto lautet, geben Sie "Admin1" ein.

      − Benutzer von relationalen Datenbanken geben den Wert, der dem bekannten Attribut %USER_ID% in der Verzeichniskonfigurationsdatei zugeordnet ist, oder die eindeutige Kennung für den Benutzer ein.

   Klicken Sie auf "Validieren", um die vollständige Kennung des Benutzers anzuzeigen.

9. Wählen Sie die Aufgaben und Rollen aus, die für diese Umgebung erstellt werden sollen. Sie können die folgenden Aufgaben ausführen:

   ■ **Create default roles (Standardrollen erstellen)**

     Erstellt einen Satz von Standardaufgaben und -rollen, die in der Umgebung verfügbar sind. Administratoren können diese Aufgaben und Rollen als Vorlagen verwenden, um neue Aufgaben und Rollen in der Benutzerkonsole zu erstellen.

- **Create only the system manager role (Nur die Rolle des Systemmanagers erstellen)**

  Erstellt nur die Rolle des Systemmanagers und die der Rolle zugeordneten Aufgaben.

  Die Rolle des Systemmanagers ist erforderlich, um auf die Umgebung zuzugreifen.

  Ein Systemmanager kann neue Aufgaben und Rollen in der Benutzerkonsole erstellen.

- **Import roles from the file (Rollen aus der Datei importieren)**

  Importiert eine Rollendefinitionsdatei, die Sie aus einer anderen CA IdentityMinder-Umgebung exportiert haben.

  **Hinweis:** Damit die CA IdentityMinder-Umgebung verwendet werden kann, muss die Rollendefinitionsdatei mindestens die Rolle des Systemmanagers oder eine Rolle mit ähnlichen Aufgaben umfassen.

  Wählen Sie die Optionsschaltfläche "Import roles from the file" (Rollen aus der Datei importieren) aus, und geben Sie den Pfad und Dateinamen der Rollendefinitionsdatei ein oder suchen Sie nach der zu importierenden Datei.

10. Wählen Sie Rollendefinitionsdateien aus, um Sätze von Standardaufgaben für Ihre Umgebung zu erstellen, und klicken Sie auf "Weiter".

    Rollendefinitionsdateien sind XML-Dateien, die einen Satz von Aufgaben und Rollen definieren, die für die Unterstützung bestimmter Funktionen erforderlich sind. Wenn Sie zum Beispiel Active Directory- und UNIX NIS-Endpunkte verwalten möchten, wählen Sie die entsprechenden Rollendefinitionsdateien aus.

    **Hinweis:** Dieser Schritt ist optional. Wenn Sie keine zusätzlichen Standardaufgaben zur Unterstützung neuer Funktionen erstellen möchten, überspringen Sie dieses Fenster.

11. Definieren Sie einen Benutzer als Systemmanager für diese Umgebung wie folgt:

    a. Geben Sie im Feld "System Manager" (Systemmanager) den Wert ein, der dem bekannten Attribut %USER_ID% in der Verzeichniskonfigurationsdatei zugeordnet ist, oder geben Sie eins der folgenden Benutzerkonten an:

       - LDAP-Benutzer geben die eindeutige Kennung oder den zugehörigen DN des Benutzers ein. Wenn der DN des Benutzer-DN zum Beispiel uid=Admin1, ou=People, ou=Employees, ou=NeteAuto lautet, geben Sie "Admin1" ein.

       - Benutzer von relationalen Datenbanken geben die eindeutige Kennung für den Benutzer ein.

b. Klicken Sie auf "Hinzufügen".

   CA IdentityMinder fügt die vollständige Kennung des Benutzers in der Liste mit Benutzern hinzu.

c. Klicken Sie auf "Weiter".

Beachten Sie beim Festlegen des Systemmanagers Folgendes:

- Der Systemmanager darf *nicht* der gleiche Benutzer wie der Administrator des Benutzerspeichers sein.
- Sie können mehrere Systemmanager für die Umgebung angeben. Sie können jedoch nur den ersten Systemmanager in der Management-Konsole angeben. Um zusätzliche Systemmanager festzulegen, weisen Sie den entsprechenden Benutzern die Rolle des Systemmanagers in der Benutzerkonsole zu.

12. Geben Sie im Feld "Inbound Administrator" (Administrator für Eingehendes) ein CA IdentityMinder-Administratorkonto an, das Admin-Aufgaben ausführen kann, die eingehenden Zuordnungen zugeordnet sind.

    Der Benutzer muss alle diese Aufgaben für einen beliebigen Benutzer ausführen können. Die Rolle "Manager für Bereitstellungssynchronisierung" enthält die Bereitstellungsaufgaben, die in den eingehenden Standardzuordnungen enthalten sind.

13. Geben Sie ein Kennwort für den Schlüsselspeicher ein. Dabei handelt es sich um die Datenbank mit Schlüsseln, die zum Verschlüsseln und Entschlüsseln von Daten verwendet werden.

    Die Definition dieses Kennworts ist eine Voraussetzung für das Definieren dynamischer Schlüssel. Sie können das Kennwort ändern, nachdem Sie die Umgebung mithilfe der Aufgaben "System", "Geheime Schlüssel" erstellt haben.

    Eine Seite wird angezeigt, auf der die Einstellungen für die Umgebung zusammengefasst werden.

14. Überprüfen Sie die Einstellungen für die Umgebung. Klicken Sie auf "Vorherige", um die Einstellungen zu ändern, oder auf "Fertig stellen", um die CA IdentityMinder-Umgebung mit den aktuellen Einstellungen zu erstellen.

    Im Fenster "Environment Configuration Output" (Umgebungskonfigurations-Ausgabe) wird der Verlauf der Umgebungserstellung angezeigt.

15. Klicken Sie auf "Fortfahren", um den CA IdentityMinder-Umgebungsassistenten zu beenden.

16. Starten Sie die Umgebung.

    Klicken Sie auf den Namen der Umgebung und anschließend auf "Starten".

17. Wenn Sie in Schritt 1 Richtlinienserver beendet haben, starten Sie diese jetzt neu.

# Zugreifen auf eine CA IdentityMinder-Umgebung

Nachdem Sie eine CA IdentityMinder-Umgebung erstellt haben, können Sie darauf zugreifen, indem Sie eine URL in einem Browser eingeben.

**Hinweis**: Aktivieren Sie JavaScript in dem Browser, den Sie verwenden, um auf die Management-Konsole zuzugreifen.

Das Format der URL hängt davon ab, wie Sie die Umgebung konfiguriert haben, und auf welche Art von Aufgabe Sie zugreifen möchten.

- Um über die Benutzerkonsole auf geschützte Aufgaben zuzugreifen, verwenden Sie die folgenden URL:

  `http://`*`Hostname`*`/iam/im/`*`alias`*

  ***Hostname***

  Definiert den vollqualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist - zum Beispiel myserver.mycompany.com.

  ***alias***

  Definiert den Alias des Umgebungs-Alias, zum Beispiel employees.

  Melden Sie sich bei der CA IdentityMinder-Umgebung mit einem privilegierten Administratorkonto an, zum Beispiel mit dem Systemmanager-Konto, das Sie für die CA IdentityMinder-Umgebung erstellt haben.

  **Hinweis:** Alle CA IdentityMinder-Aufgaben sind geschützt, außer wenn Sie öffentliche Aufgaben konfigurieren.

- Um auf öffentliche Aufgaben zuzugreifen, für die Benutzer keine Anmeldeinformationen angeben müssen, verwenden Sie eine URL mit dem folgenden Format:

  `http://`*`Hostname`*`/iam/im/`*`alias`*`/index.jsp?task.tag=`*`tasktag`*

  ***Hostname***

  Definiert den vollqualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist, zum Beispiel myserver.mycompany.com.

***alias***

Definiert den Alias für öffentliche Aufgaben, zum Beispiel Self-Service.

***task_tag***

Definiert das Tag, dass die Aufgabe startet.

Sie geben das Aufgaben-Tag an, wenn Sie eine Aufgabe in der Benutzerkonsole konfigurieren.

Die Aufgaben-Tags für die Standardaufgaben für die Selbstregistrierung und das Zurücksetzen vergessener Kennwörter sind "SelfRegistration" und "ForgottenPasswordReset".

**Hinweis:** Weitere Informationen finden Sie im *Administrationshandbuch*.

# Konfigurieren einer Umgebung für die Bereitstellung

Sie können eine Umgebung für die Bereitstellung konfigurieren, nachdem Sie den Zugriff auf den Bereitstellungsserver aktiviert haben (siehe Seite 174).

Erstellen Sie dann einen besonderen CA IdentityMinder-Benutzer, der als "Inbound Administrator" (Administrator für Eingehendes) bezeichnet wird, erstellen Sie eine Verbindung mit dem Bereitstellungsserver, und konfigurieren Sie die eingehende Synchronisierung im Bereitstellungsmanager.

**Hinweis:** Immer, wenn Sie die Bereitstellungseigenschaften für eine Umgebung ändern, muss der Anwendungsserver neu gestartet werden, damit die Änderungen wirksam werden.

## Konfigurieren des Inbound Administrators (Administrator für Eingehendes)

Damit die eingehende Synchronisierung funktioniert, erstellen Sie einen besonderen CA IdentityMinder-Benutzer, der als *Inbound Administrator* bezeichnet wird. In früheren Versionen von CA IdentityMinder wurde der Inbound Administrator als *Corporate User* bezeichnet. Bei diesem Benutzerkonto meldet sich kein Benutzer an; stattdessen wird es von CA IdentityMinder intern verwendet. Erstellen Sie dieses Benutzerkonto dennoch, und ordnen Sie ihm die entsprechenden Aufgaben zu.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei der CA IdentityMinder-Umgebung als Benutzer mit der Rolle des Systemmanagers an.
2. Erstellen Sie einen Benutzer. Sie können den Benutzer zur Erinnerung an seinen Zweck **inbound** nennen.

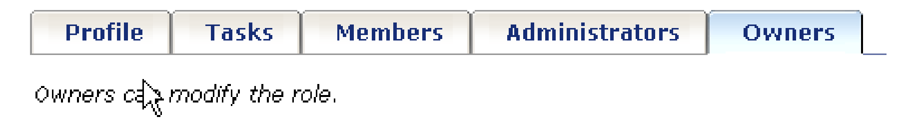
3. Wählen Sie "Admin-Rollen", "Admin-Rolle ändern" und anschließend eine Rolle aus, die die Aufgaben enthält, die Sie für die Synchronisierung verwenden.

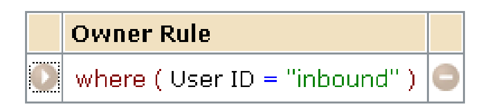
   - Bereitstellung: Benutzer erstellen
   - Provisioning Enable/Disable User (Bereitstellung: Benutzer aktivieren/deaktivieren)
   - Bereitstellung: Benutzer ändern

   **Hinweis:** Wenn Sie die Standardsynchronisierungsaufgaben nicht geändert haben, verwenden Sie die Rolle "Manager für Bereitstellungssynchronisierung".

4. Fügen Sie auf der Registerkarte "Mitglieder" eine Mitgliederrichtlinie hinzu, die Folgendes einschließt:

   - Ein Mitgliederregel, welcher der neue Benutzer entspricht.
   - Eine Umfangsregel, die allen Benutzern Zugriff gibt, die von Änderungen am Bereitstellungsverzeichnis betroffen sind, die eine eingehende Synchronisierung auslösen.




5. In der Managementkonsole:

   a. Wählen Sie die Umgebung aus.

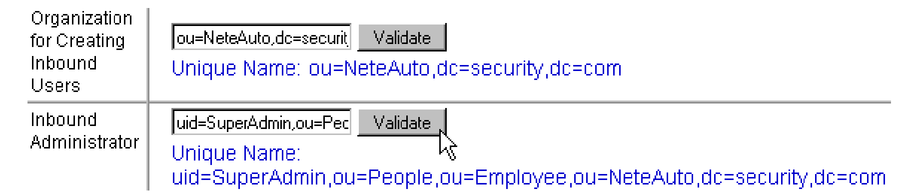
   b. Wählen Sie "Advanced Settings" (Erweiterte Einstellungen), "Provisioning" (Bereitstellung) aus.

   c. Geben Sie die Organisation für das Feld "Creating Inbound Users" (Eingehende Benutzer erstellen) ein, wenn das CA IdentityMinder-Verzeichnis eine Organisation enthält.

      Diese Organisation ist diejenige, in der Benutzer erstellt werden, wenn eingehende Synchronisierung auftritt. Wenn zum Beispiel ein Benutzer im Bereitstellungsverzeichnis hinzugefügt wird, fügt CA IdentityMinder den Benutzer zu dieser Organisation hinzu.

d. Geben Sie in das Feld (Administrator für Eingehendes) die Benutzer-ID des Benutzers ein, den Sie in Schritt 2 erstellt haben.

e. Klicken Sie auf "Validieren", um zu bestätigen, dass die Benutzer-ID akzeptiert wurde - wie im folgenden Beispiel zu sehen ist, in dem die vollständige Benutzer-ID unter der eingegebenen Benutzer-ID angezeigt wird.




f. Ändern Sie andere Felder in diesem Fenster. Keine Änderungen sind erforderlich.

Ändern Sie nur etwas, wenn Sie verstehen, wie die Felder interagieren. Um Details zu jedem Feld zu erhalten, klicken Sie auf die Hilfeverknüpfung in dem Fenster.

## Herstellen einer Verbindung zwischen der Umgebung und dem Bereitstellungsserver

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste der vorhandenen Umgebungen wird angezeigt.

2. Klicken Sie auf den Namen der Umgebung, die Sie dem Bereitstellungsserver zuordnen möchten.

3. Klicken Sie im Feld "Bereitstellungsserver" auf das Symbol mit dem Rechtspfeil.

   Das Fenster "Provisioning Properties" (Bereitstellungseigenschaften) wird geöffnet.

4. Wählen Sie den gewünschten Bereitstellungsserver aus.

5. Klicken Sie im unteren Bereich des Fensters auf "Speichern".

6. Konfigurieren Sie die Synchronisierung im Bereitstellungsmanager (siehe Seite 201).

## Konfigurieren der Synchronisierung im Bereitstellungsmanager

Eingehende Synchronisierung hält CA IdentityMinder im Hinblick auf Änderungen auf dem Laufenden, die im Bereitstellungsverzeichnis auftreten. Zu den Änderungen gehören diejenigen, die mithilfe des Bereitstellungsmanagers vorgenommen wurden, und Änderungen in Endpunkten, für die der Bereitstellungsserver einen Connector hat. Jeder Bereitstellungsserver unterstützt eine einzelne Umgebung. Sie können jedoch Sicherungsumgebungen auf unterschiedlichen Systemen in einem Cluster konfigurieren, falls die aktuelle Umgebung nicht verfügbar ist.

**Gehen Sie wie folgt vor:**

1. Wählen Sie "Start", "CA Identity Manager", "Bereitstellungsmanager".
2. Klicken Sie auf "System"," CA IdentityMinder Setup".
3. Geben Sie im Feld "Hostname" den Namen des Systems an, auf dem der CA IdentityMinder-Server installiert ist.
4. Geben Sie im Feld "Port" die Portnummer des Anwendungsservers ein.
5. Geben Sie im Feld "Environment name" (Umgebungsname) den Alias für die Umgebung ein.
6. Wählen Sie "Gesicherte Verbindung" aus, wenn Sie das HTTPS-Protokoll für die Kommunikation mit dem CA IdentityMinder-Server verwenden möchten, statt das HTTP-Protokoll zu verwenden und die einzelnen Benachrichtigungen zu verschlüsseln.
7. Klicken Sie auf "Hinzufügen".
8. Wiederholen Sie die Schritte 3-6 für jede Sicherungsversion der Umgebung.

   Wenn der Anwendungsserver für die aktuelle Umgebung nicht verfügbar ist, wird CA IdentityMinder in einer Sicherungsumgebung ausgeführt. Sie können die aktuelle Umgebung und die Sicherungsumgebungen neu anordnen, um die Reihenfolge für den Failover-Befehl festzulegen.
9. Wenn es sich um die erste Umgebung handelt, geben Sie in die Felder "Gemeinsamer geheimer Schlüssel" das Kennwort ein, das während der CA IdentityMinder-Installation für den Benutzer für eingebettete Komponenten eingegeben wurde.

   **Hinweis**: Diese Felder gelten nicht, wenn FIPS in dieser Installation aktiviert ist.
10. Legen Sie die Protokollebene folgendermaßen fest:
    - Kein Protokoll - Keine Informationen werden in die Protokolldatei geschrieben.
    - Fehler - Es werden nur Fehlermeldungen protokolliert.
    - Info - Fehler- und Informationsmeldungen werden protokolliert (Standard).
    - Warnung - Fehler-, Warn- und Informationsmeldungen werden protokolliert.
    - Debug - Alle Informationen werden protokolliert.
11. Starten Sie den Anwendungsserver neu, bevor Sie sich bei der Umgebung anmelden.

**Hinweis**: Ein Protokoll zu eingehenden Synchronisierungsvorgängen und allen Problemen, die während der Synchronisierung aufgetreten sind, finden Sie in der folgenden Datei:

*PSHOME*\logs\etanotify<Datum>.log

## Importieren von benutzerdefinierten Bereitstellungsrollen

Wenn Sie die Umgebung erstellen, können Sie die Standardrollen oder eine benutzerdefinierte Rollendefinitionsdatei verwenden, die Sie erstellen. Wenn Sie benutzerdefinierte Rollendefinitionen importieren, importieren Sie *auch* die Rollendefinitionen, die ausschließlich für die Bereitstellung gelten. Nachdem Sie die Umgebung erstellt haben, importieren Sie die Rollendefinitionen aus der Datei "ProvisioningOnly-RoleDefinitions.xml", die sich in einem der folgenden Ordner befindet:

*admin_tools*/ProvisioningOnlyRoleDefinitions/Organization
*admin_tools*/ProvisioningOnlyRoleDefinitions/NoOrganization

Der Standardspeicherort für *admin_tools* ist:

- **Windows**: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

## Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen"

Um die Bereitstellung für eine CA IdentityMinder-Umgebung zu aktivieren, importieren Sie eine Konfigurationsdatei namens ProvisioningOnly-RoleDefinitions.xml, die die Rollen und Aufgaben für die Benutzereinrichtung erstellt.

In dieser Datei ist die Standardeinstellung der Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen" deaktiviert. (Bevor Sie die Bereitstellung aktivieren, ist die Synchronisierungseinstellung auf "Bei Abschluss der Aufgabe" gesetzt.)

Um durch das Zurücksetzen des Benutzerkennworts eine Kontosynchronisierung auszulösen, stellen Sie die Kontosynchronisierungsoption ein, nachdem Sie die Datei ProvisioningOnly-RoleDefinitions.xml importiert haben, um die Bereitstellung zu aktivieren.

## So können Sie Connectors mithilfe von Connector Xpress erstellen und bereitstellen

Sie können die Bereitstellung für eine Umgebung konfigurieren, um Konten in anderen Systemen für Benutzer bereitzustellen, die von CA IdentityMinder verwaltet werden. Konten bieten Benutzern Zugriff auf zusätzliche Ressourcen, wie ein E-Mail-Konto. Sie geben diese zusätzlichen Konten an, indem Sie die Bereitstellungsrollen zuweisen, die Sie über CA IdentityMinder erstellen.

**Konfigurieren einer Umgebung für die Bereitstellung**

System-
administrator

Voraussetzungen überprüfen

Bereitstellungs-server-Zugriff aktivieren

Inbound Administrator konfigurieren

Verbindung zwischen einer Umgebung und dem Bereitstellungsserver herstellen

Synchronisierung im Bereitstellungs-manager konfigurieren

Benutzerdefinierte Bereitstellungsrollen importieren

Kontensynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen"

Stellen Sie als Administrator folgende Schritte fertig:

1. Überprüfen der Voraussetzungen (siehe Seite 205)

2. Aktivieren von Bereitstellungsserver-Zugriff (siehe Seite 174)
3. Konfigurieren des Inbound Administrators (Administrator für Eingehendes) (siehe Seite 199)
4. Herstellen einer Verbindung zwischen der Umgebung und dem Bereitstellungsserver (siehe Seite 201)
5. Konfigurieren der Synchronisierung im Bereitstellungsmanager (siehe Seite 201)
6. Importieren von benutzerdefinierten Bereitstellungsrollen (siehe Seite 203)
7. Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen" (siehe Seite 203)

## Überprüfen der Voraussetzungen

Bevor Sie die Umgebung für die Bereitstellung konfigurieren, stellen Sie sicher, dass das Bereitstellungsverzeichnis auf CA Directory installiert ist. Weitere Informationen dazu finden Sie im *Installationshandbuch*.

## Aktivieren von Bereitstellungsserver-Zugriff

Sie aktivieren den Zugriff auf den Bereitstellungsserver durch die Verwendung des Links "Directories" (Verzeichnisse) in der Management-Konsole.

**Hinweis**: Eine Voraussetzung für diesen Vorgang ist, das Bereitstellungsverzeichnis auf CA Directory zu installieren. Weitere Informationen dazu finden Sie im *Installationshandbuch*.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Management-Konsole, indem Sie die folgende URL in einen Browser eingeben:

   http://*hostname*:*port*/iam/immanage

   *Hostname*

   Definiert den voll qualifizierten Hostnamen des Systems, auf dem der CA IdentityMinder-Server installiert ist.

   *port*

   Definiert die Portnummer des Anwendungsservers.

2. Klicken Sie auf "Directories" (Verzeichnisse).

   Das CA IdentityMinder-Verzeichnisfenster wird geöffnet.

3. Klicken Sie auf "Create from Wizard" (Über Assistenten erstellen).

4. Geben Sie den Pfad und Dateinamen der Verzeichnis-XML-Datei für das Konfigurieren des Bereitstellungsverzeichnisses ein. Es wird unter "directoryTemplates\ProvisioningServer" im Ordner "Verwaltung" gespeichert. Der Standardspeicherort dieses Ordners ist:

   - Windows: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   **Hinweis:** Sie können diese Verzeichniskonfigurationsdatei wie installiert ohne Änderungen verwenden.

5. Klicken Sie auf "Weiter".

6. Geben Sie Werte für die Felder in diesem Fenster folgendermaßen an:

   **Name**

   Ist ein Name für das Bereitstellungsverzeichnis, das dem Bereitstellungsserver zugeordnet wird, den Sie konfigurieren.

   - Wenn CA IdentityMinder nicht in SiteMinder integriert ist, geben Sie einen aussagekräftigen Namen für das Objekt an, das CA IdentityMinder verwendet, um mit dem Benutzerverzeichnis Verbindung aufzunehmen.
   - Wenn CA IdentityMinder in SiteMinder integriert ist, haben Sie zwei Optionen:

     Wenn Sie ein Benutzerverzeichnis-Verbindungsobjekt in SiteMinder erstellen wollen, geben Sie einen aussagekräftigen Namen an. CA IdentityMinder erstellt dieses Objekt in SiteMinder mit dem Namen, den Sie angeben.

     Wenn Sie mit einem vorhandenen SiteMinder-Benutzerverzeichnis Verbindung aufnehmen wollen, geben Sie den Namen des SiteMinder-Benutzerverzeichnis-Verbindungsobjekts genau an, wie er in der Richtlinienserver-Benutzeroberfläche angezeigt wird.

   **Beschreibung**

   (Optional) Beschreibt das CA IdentityMinder-Verzeichnis.

   **Host**

   Gibt den Hostnamen oder die IP-Adresse des Servers an, auf dem das Benutzerverzeichnis installiert ist.

   **Port**

   Gibt die Portnummer des Benutzerverzeichnisses an.

**Domäne**

Gibt den Namen der Bereitstellungsdomäne an, die CA IdentityMinder verwaltet.

**Wichtig!** Wenn Sie ein Bereitstellungsverzeichnis über die Management-Konsole mit fremdsprachigen Zeichen als Domänenname erstellen, schlägt die Bereitstellungsverzeichnis-Erstellung fehl.

Der Name muss mit dem Namen der Bereitstellungsdomäne übereinstimmen, den Sie während Installation angaben.

**Hinweis:** Der Domänenname berücksichtigt Groß- und Kleinschreibung.

**Benutzername**

Gibt einen Benutzer an, der sich beim Bereitstellungsmanager anmelden kann.

Der Benutzer muss das Domänenadministrator-Profil oder ein gleichwertiges Set von Berechtigungen für die Bereitstellungsdomäne haben.

**Kennwort**

Gibt das Kennwort für den globalen Benutzer an, den Sie im Feld "Benutzername" angegeben haben.

**Kennwort bestätigen**

Geben Sie das in das Feld "Kennwort" eingegebene Kennwort erneut zur Bestätigung ein.

**Sichere Verbindung**

Zeigt an, ob CA IdentityMinder eine sichere Verbindung verwendet.

Wählen Sie diese Option für Active Directory-Benutzerspeicher aus.

**Verzeichnissuchparameter**

**maxrows** definiert die Höchstanzahl von Ergebnissen, die CA IdentityMinder zurückgeben kann, wenn man ein Benutzerverzeichnis durchsucht. Dieser Wert überschreibt ein im LDAP-Verzeichnis festgelegtes Limit. Wenn diese im Gegensatz stehen, verwendet der LDAP-Server die niedrigste Einstellung.

**Hinweis:** Der maxrows-Parameter beschränkt nicht die Anzahl von Ergebnissen, die im CA IdentityMinder-Aufgabenfenster angezeigt werden. Um die Anzeigeeinstellungen zu konfigurieren, ändern Sie die Listenfensterdefinition in der CA IdentityMinder-Benutzerkonsole. Weitere Anweisungen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**timeout** bestimmt die maximale Anzahl von Sekunden, die CA IdentityMinder ein Verzeichnis durchsucht, bevor es die Suche beendet.

**Failover-Verbindungen**

Hostname und Portnummer von einem oder mehreren optionalen Systemen, die alternative Bereitstellungsserver sind. Wenn mehrere Server aufgelistet sind, versucht CA IdentityMinder, mit den Systemen in der Reihenfolge Verbindung aufzunehmen, in der sie aufgelistet sind.

Die alternativen Bereitstellungsserver werden verwendet, wenn der primäre Bereitstellungsserver fehlschlägt. Wenn der primäre Bereitstellungsserver erneut verfügbar wird, wird der alternative Bereitstellungsserver weiterhin verwendet. Wenn Sie zur Verwendung des Bereitstellungsservers zurückkehren möchten, starten Sie den alternativen Bereitstellungsserver neu.

7. Klicken Sie auf "Weiter".
8. Wählen Sie die zu verwaltenden Objekte aus, wie Benutzer oder Gruppen.
9. Nachdem Sie die Objekte nach Bedarf konfiguriert haben, lassen Sie die Zusammenfassung der Bereitstellung des Verzeichnisses anzeigen und überprüfen die Einstellungen für das Bereitstellungsverzeichnis.
10. Klicken Sie auf eine dieser Aktionen:
    a. Klicken Sie auf "Zurück", um etwas zu ändern.
    b. Klicken Sie auf "Speichern", um die Verzeichnisinformationen zu speichern, wenn Sie später zur Bereitstellung zurückkommen wollen.
    c. Klicken Sie auf "Fertig stellen", um diesen Vorgang abzuschließen und anzufangen, eine Umgebung für die Bereitstellung zu konfigurieren (siehe Seite 199).

## Konfigurieren des Inbound Administrators (Administrator für Eingehendes)

Damit die eingehende Synchronisierung funktioniert, erstellen Sie einen besonderen CA IdentityMinder-Benutzer, der als *Inbound Administrator* bezeichnet wird. In früheren Versionen von CA IdentityMinder wurde der Inbound Administrator als *Corporate User* bezeichnet. Bei diesem Benutzerkonto meldet sich kein Benutzer an; stattdessen wird es von CA IdentityMinder intern verwendet. Erstellen Sie dieses Benutzerkonto dennoch, und ordnen Sie ihm die entsprechenden Aufgaben zu.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei der CA IdentityMinder-Umgebung als Benutzer mit der Rolle des Systemmanagers an.
2. Erstellen Sie einen Benutzer. Sie können den Benutzer zur Erinnerung an seinen Zweck **inbound** nennen.

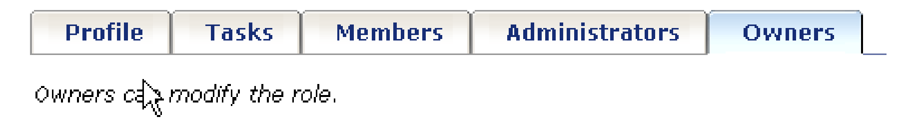
3. Wählen Sie "Admin-Rollen", "Admin-Rolle ändern" und anschließend eine Rolle aus, die die Aufgaben enthält, die Sie für die Synchronisierung verwenden.

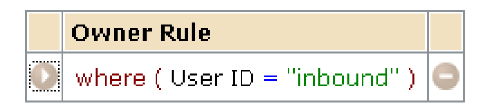
   - Bereitstellung: Benutzer erstellen
   - Provisioning Enable/Disable User (Bereitstellung: Benutzer aktivieren/deaktivieren)
   - Bereitstellung: Benutzer ändern

   **Hinweis:** Wenn Sie die Standardsynchronisierungsaufgaben nicht geändert haben, verwenden Sie die Rolle "Manager für Bereitstellungssynchronisierung".

4. Fügen Sie auf der Registerkarte "Mitglieder" eine Mitgliederrichtlinie hinzu, die Folgendes einschließt:

   - Ein Mitgliederregel, welcher der neue Benutzer entspricht.
   - Eine Umfangsregel, die allen Benutzern Zugriff gibt, die von Änderungen am Bereitstellungsverzeichnis betroffen sind, die eine eingehende Synchronisierung auslösen.




5. In der Managementkonsole:

   a. Wählen Sie die Umgebung aus.

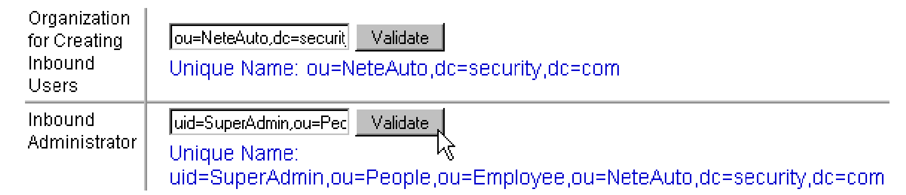
   b. Wählen Sie "Advanced Settings" (Erweiterte Einstellungen), "Provisioning" (Bereitstellung) aus.

   c. Geben Sie die Organisation für das Feld "Creating Inbound Users" (Eingehende Benutzer erstellen) ein, wenn das CA IdentityMinder-Verzeichnis eine Organisation enthält.

   Diese Organisation ist diejenige, in der Benutzer erstellt werden, wenn eingehende Synchronisierung auftritt. Wenn zum Beispiel ein Benutzer im Bereitstellungsverzeichnis hinzugefügt wird, fügt CA IdentityMinder den Benutzer zu dieser Organisation hinzu.

d. Geben Sie in das Feld (Administrator für Eingehendes) die Benutzer-ID des Benutzers ein, den Sie in Schritt 2 erstellt haben.

e. Klicken Sie auf "Validieren", um zu bestätigen, dass die Benutzer-ID akzeptiert wurde - wie im folgenden Beispiel zu sehen ist, in dem die vollständige Benutzer-ID unter der eingegebenen Benutzer-ID angezeigt wird.




f. Ändern Sie andere Felder in diesem Fenster. Keine Änderungen sind erforderlich.

Ändern Sie nur etwas, wenn Sie verstehen, wie die Felder interagieren. Um Details zu jedem Feld zu erhalten, klicken Sie auf die Hilfeverknüpfung in dem Fenster.

## Herstellen einer Verbindung zwischen der Umgebung und dem Bereitstellungsserver

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste der vorhandenen Umgebungen wird angezeigt.

2. Klicken Sie auf den Namen der Umgebung, die Sie dem Bereitstellungsserver zuordnen möchten.

3. Klicken Sie im Feld "Bereitstellungsserver" auf das Symbol mit dem Rechtspfeil.

   Das Fenster "Provisioning Properties" (Bereitstellungseigenschaften) wird geöffnet.

4. Wählen Sie den gewünschten Bereitstellungsserver aus.

5. Klicken Sie im unteren Bereich des Fensters auf "Speichern".

6. Konfigurieren Sie die Synchronisierung im Bereitstellungsmanager (siehe Seite 201).

## Konfigurieren der Synchronisierung im Bereitstellungsmanager

Eingehende Synchronisierung hält CA IdentityMinder im Hinblick auf Änderungen auf dem Laufenden, die im Bereitstellungsverzeichnis auftreten. Zu den Änderungen gehören diejenigen, die mithilfe des Bereitstellungsmanagers vorgenommen wurden, und Änderungen in Endpunkten, für die der Bereitstellungsserver einen Connector hat. Jeder Bereitstellungsserver unterstützt eine einzelne Umgebung. Sie können jedoch Sicherungsumgebungen auf unterschiedlichen Systemen in einem Cluster konfigurieren, falls die aktuelle Umgebung nicht verfügbar ist.

**Gehen Sie wie folgt vor:**

1. Wählen Sie "Start", "CA Identity Manager", "Bereitstellungsmanager".
2. Klicken Sie auf "System"," CA IdentityMinder Setup".
3. Geben Sie im Feld "Hostname" den Namen des Systems an, auf dem der CA IdentityMinder-Server installiert ist.
4. Geben Sie im Feld "Port" die Portnummer des Anwendungsservers ein.
5. Geben Sie im Feld "Environment name" (Umgebungsname) den Alias für die Umgebung ein.
6. Wählen Sie "Gesicherte Verbindung" aus, wenn Sie das HTTPS-Protokoll für die Kommunikation mit dem CA IdentityMinder-Server verwenden möchten, statt das HTTP-Protokoll zu verwenden und die einzelnen Benachrichtigungen zu verschlüsseln.
7. Klicken Sie auf "Hinzufügen".
8. Wiederholen Sie die Schritte 3-6 für jede Sicherungsversion der Umgebung.

   Wenn der Anwendungsserver für die aktuelle Umgebung nicht verfügbar ist, wird CA IdentityMinder in einer Sicherungsumgebung ausgeführt. Sie können die aktuelle Umgebung und die Sicherungsumgebungen neu anordnen, um die Reihenfolge für den Failover-Befehl festzulegen.
9. Wenn es sich um die erste Umgebung handelt, geben Sie in die Felder "Gemeinsamer geheimer Schlüssel" das Kennwort ein, das während der CA IdentityMinder-Installation für den Benutzer für eingebettete Komponenten eingegeben wurde.

   **Hinweis**: Diese Felder gelten nicht, wenn FIPS in dieser Installation aktiviert ist.
10. Legen Sie die Protokollebene folgendermaßen fest:
    - Kein Protokoll - Keine Informationen werden in die Protokolldatei geschrieben.
    - Fehler - Es werden nur Fehlermeldungen protokolliert.
    - Info - Fehler- und Informationsmeldungen werden protokolliert (Standard).
    - Warnung - Fehler-, Warn- und Informationsmeldungen werden protokolliert.
    - Debug - Alle Informationen werden protokolliert.
11. Starten Sie den Anwendungsserver neu, bevor Sie sich bei der Umgebung anmelden.

**Hinweis**: Ein Protokoll zu eingehenden Synchronisierungsvorgängen und allen Problemen, die während der Synchronisierung aufgetreten sind, finden Sie in der folgenden Datei:

*PSHOME*\logs\etanotify<Datum>.log

### Importieren von benutzerdefinierten Bereitstellungsrollen

Wenn Sie die Umgebung erstellen, können Sie die Standardrollen oder eine benutzerdefinierte Rollendefinitionsdatei verwenden, die Sie erstellen. Wenn Sie benutzerdefinierte Rollendefinitionen importieren, importieren Sie *auch* die Rollendefinitionen, die ausschließlich für die Bereitstellung gelten. Nachdem Sie die Umgebung erstellt haben, importieren Sie die Rollendefinitionen aus der Datei "ProvisioningOnly-RoleDefinitions.xml", die sich in einem der folgenden Ordner befindet:

*admin_tools*/ProvisioningOnlyRoleDefinitions/Organization
*admin_tools*/ProvisioningOnlyRoleDefinitions/NoOrganization

Der Standardspeicherort für *admin_tools* ist:

- **Windows**: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

### Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen"

Um die Bereitstellung für eine CA IdentityMinder-Umgebung zu aktivieren, importieren Sie eine Konfigurationsdatei namens ProvisioningOnly-RoleDefinitions.xml, die die Rollen und Aufgaben für die Benutzereinrichtung erstellt.

In dieser Datei ist die Standardeinstellung der Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen" deaktiviert. (Bevor Sie die Bereitstellung aktivieren, ist die Synchronisierungseinstellung auf "Bei Abschluss der Aufgabe" gesetzt.)

Um durch das Zurücksetzen des Benutzerkennworts eine Kontosynchronisierung auszulösen, stellen Sie die Kontosynchronisierungsoption ein, nachdem Sie die Datei ProvisioningOnly-RoleDefinitions.xml importiert haben, um die Bereitstellung zu aktivieren.

## Verwalten von Umgebungen

In diesem Abschnitt wird die Verwaltung einer Umgebung beschrieben.

### Ändern von CA IdentityMinder-Umgebungseigenschaften

Im Fenster "CA IdentityMinder Environment Properties" (Umgebungseigenschaften) in der Management-Konsole können Sie die folgenden Aufgaben ausführen:

- Zeigen Sie die aktuellen Einstellungen für die Umgebung an.
- Ändern Sie die Beschreibung, die Basis-URL sowie geschützte und öffentliche Aliasnamen.

- Importieren Sie nach einem Upgrade eine vorhandene CA IdentityMinder-Umgebung.

  **Hinweis:** Weitere Informationen zum Importieren vorhandener CA IdentityMinder-Umgebungen finden Sie im Abschnitt zu Upgrades im *Installationshandbuch*.

- Starten und Anhalten von Umgebungen
- Seiten für den Zugriff, um die folgenden Aufgaben zu konfigurieren:
  - **Erweiterte Einstellungen**

    Konfiguriert erweiterte Funktionen, einschließlich Funktionen, die mithilfe der CA IdentityMinder-APIs erstellt werden.

  - **Role and Task Settings (Rollen- und Aufgabeneinstellungen)**

    Importiert eine Rollendefinitionsdatei, die Sie aus einer anderen CA IdentityMinder-Umgebung exportiert haben.

  - **System Manager (Systemmanager)**

    Weist Systemmanager-Rollen zu.

**Gehen Sie wie folgt vor:**

1. Wenn CA IdentityMinder einen SiteMinder-Richtlinienserver-Cluster verwendet, beenden Sie alle bis auf einen Richtlinienserver.
2. Wenn Sie einen Cluster von CA IdentityMinder-Knoten haben, beenden Sie alle bis auf einen CA IdentityMinder-Knoten.
3. Klicken Sie auf "Umgebungen".

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

4. Klicken Sie auf den Namen der zu ändernden CA IdentityMinder-Umgebung.

   Das Fenster "CA IdentityMinder Properties" (Eigenschaften) wird mit den folgenden Eigenschaften angezeigt:

   **OID**

   Gibt eine eindeutige Kennung für die Umgebung an. CA IdentityMinder generiert diese Kennung, wenn Sie eine CA IdentityMinder-Umgebung erstellen.

   Sie verwenden die OID, wenn Sie das Entfernen einer Aufgabe aus einer Aufgabenpersistenz-Datenbank konfigurieren. Weitere Informationen hierzu finden Sie im *Installationshandbuch*.

   **Name**

   Gibt den eindeutigen Namen der CA IdentityMinder-Umgebung an.

**Beschreibung**

Gibt eine Beschreibung der CA IdentityMinder-Umgebung an.

**CA IdentityMinder-Verzeichnis**

Gibt das CA IdentityMinder-Verzeichnis an, dem die Umgebung zugeordnet ist.

**Enable Verbose Log Output (Ausführliche Protokollierungsausgabe aktivieren)**

Steuert, wie viele Informationen CA IdentityMinder im Umgebungsprotokoll aufzeichnet und anzeigt, wenn Sie eine Umgebung importieren. Das Umgebungsprotokoll wird im Statusfenster in der Management-Konsole angezeigt, wenn Sie eine Umgebung oder andere Objektdefinitionen aus einer Datei importieren.

**Hinweis:** Wenn Sie dieses Kontrollkästchen aktivieren, kann sich dies beträchtlich auf die Leistung auswirken.

Das ausführliche Protokoll schließt Validierungs- und Bereitstellungsmeldungen für jedes Objekt (Aufgabe, Fenster, Rolle und Richtlinie) und die zugehörigen Attribute in der Umgebung ein.

Um das ausführliche Protokoll anzuzeigen, aktivieren Sie dieses Kontrollkästchen, und speichern Sie die Umgebungseigenschaften. Wenn Sie Rollen oder andere Einstellungen aus einer Datei importieren, werden die zusätzlichen Informationen im Protokoll angezeigt.

**Bereitstellungsserver**

Gibt das Bereitstellungsverzeichnis an, das als Benutzerspeicher für die Bereitstellung verwendet wird.

Klicken Sie auf die Schaltfläche mit dem Rechtspfeil, um das Bereitstellungsverzeichnis auf der Seite "Provisioning Properties" (Bereitstellungseigenschaften) zu konfigurieren.

**Version**

Definiert die Versionsnummer von CA IdentityMinder.

**Base URL (Basis-DN)**

Gibt den Teil der CA IdentityMinder-URL an, die nicht den geschützten oder öffentlichen Alias für die Umgebung enthält.

CA IdentityMinder verwendet die Basis-URL für die Bildung der Umleitungs-URL, die auf die Kennwortdienst-Aufgabe in der Standardkennwortrichtlinie für die Umgebung hinweist.

**Protected Alias (Geschützter Alias)**

Definiert den Namen der Basis-URL für den Zugriff auf geschützte Aufgaben in der Benutzerkonsole für eine CA IdentityMinder-Umgebung.

**Öffentliches Alias**

Definiert den Namen der Basis-URL für den Zugriff auf öffentliche Aufgaben, zum Beispiel Selbstregistrierungsaufgaben und Aufgaben in Bezug auf vergessene Kennwörter.

**Public User (Öffentlicher Benutzer)**

Definiert das Benutzerkonto, das CA IdentityMinder anstelle der Anmeldeinformationen des Benutzers für den Zugriff auf öffentliche Aufgaben verwendet.

**Job Timeout (Job-Zeitlimit)**

Bestimmt, wie lange CA IdentityMinder nach dem Übermitteln einer Aufgabe wartet, bevor eine Statusmeldung angezeigt wird.

Dieser Wert wird auf der Seite "User Console" (Benutzerkonsole) in "Erweiterte Einstellungen" festgelegt.

**Status**

Hält die CA IdentityMinder-Umgebung an oder startet sie neu.

**Migrate Task Persistence Data from CA IdentityMinder 8.1 (Aufgabenpersistenz-Daten aus CA IdentityMinder 8.1 migrieren)**

Migriert Daten aus einer CA IdentityMinder 8.1-Aufgabenpersistenz-Datenbank in eine CA IdentityMinder 12.6.3-Aufgabenpersistenz-Datenbank.

Weitere Informationen dazu finden Sie im *Installationshandbuch*.

**Hinweis:** Die Schaltfläche "Migrate Task Persistence Data from CA IdentityMinder 8.1" wird nur in Umgebungen angezeigt, die in Vorgängerversionen von CA IdentityMinder erstellt und zu CA IdentityMinder 12.6.3 migriert wurden.

5. Ändern Sie ggf. die Beschreibung, die Basis-URL oder den geschützten bzw. öffentlichen Alias.
6. Wenn Sie Umgebungseigenschaften geändert haben, starten Sie die CA IdentityMinder-Umgebung neu.
7. Wenn Sie in Schritt 1 Richtlinienserver beendet haben, starten Sie diese jetzt neu.

## Umgebungseinstellungen

Umgebungsspezifische Informationen werden in drei Dateien mit Umgebungseinstellungen gespeichert:

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

**Hinweis:** *alias* bezieht sich auf den Alias für die Umgebung. Sie geben den Alias an, wenn Sie die Umgebung erstellen.

Generieren Sie eine ZIP-Datei, die diese Dateien enthält, die die aktuelle Konfiguration widerspiegeln, wenn Sie die Umgebungseinstellungen exportieren.

Nachdem Sie die Umgebungseinstellungen exportiert haben, importieren Sie die Einstellungen, um eine der folgenden Aufgaben auszuführen:

- Sie verwalten mehrere Umgebungen mit ähnlichen Einstellungen. In diesem Fall erstellen Sie eine Umgebung mit den erforderlichen Einstellungen, importieren diese Einstellungen in andere Umgebungen, und passen dann die Einstellungen in jeder Umgebung nach Bedarf an.
- Sie migrieren eine Umgebung aus einem Entwicklungssystem in ein Produktionssystem.
- Sie aktualisieren eine vorhandene Umgebung, nachdem Sie ein Upgrade auf eine neue Version von CA IdentityMinder durchgeführt haben.

## Exportieren einer CA IdentityMinder-Umgebung

Um eine CA IdentityMinder-Umgebung auf einem Produktionssystem bereitzustellen, exportieren Sie die Umgebung aus einem Entwicklungs- oder Staging-System, und importieren Sie sie in das Produktionssystem.

**Hinweis:** Wenn Sie eine zuvor exportierte Umgebung importieren, zeigt CA IdentityMinder ein Protokoll in einem Statusfenster in der Management-Konsole an. Um Validierungs- und Bereitstellungsinformationen für jedes verwaltete Objekt und seine Attribute in diesem Protokoll anzuzeigen, wählen Sie das Feld "Enable Verbose Log Output" (Ausführliche Protokollierungsausgabe aktivieren) auf der Seite "Environment Properties" (Umgebungseigenschaften) aus, *bevor* Sie die Umgebung exportieren. Die Auswahl des Felds "Enable Verbose Log Output" kann beträchtliche Leistungsprobleme beim Importieren verursachen.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Environments" (Umgebungen).

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

2. Wählen Sie die Umgebung aus, die Sie exportieren möchten.
3. Klicken Sie auf die Schaltfläche "Exportieren".

   Ein Dateidownload-Fenster wird angezeigt.

4. Speichern Sie die ZIP-Datei an einem Speicherort, auf den das Produktionssystem zugreifen kann.
5. Klicken Sie auf "Fertig stellen".

Die Umgebungsinformationen werden in eine ZIP-Datei exportiert, die Sie in eine andere Umgebung importieren können.

## Importieren einer CA IdentityMinder-Umgebung

Sie können CA IdentityMinder-Umgebungseinstellungen importieren, um eine der folgenden Aufgaben auszuführen:

- Sie verwalten mehrere Umgebungen mit ähnlichen Einstellungen. In diesem Fall erstellen Sie eine Umgebung mit den erforderlichen Einstellungen, importieren diese Einstellungen in andere Umgebungen, und passen dann die Einstellungen in jeder Umgebung nach Bedarf an.
- Sie migrieren eine Umgebung aus einem Entwicklungssystem in ein Produktionssystem.
- Sie aktualisieren eine vorhandene Umgebung, nachdem Sie ein Upgrade auf eine neue Version von CA IdentityMinder durchgeführt haben.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Environments" (Umgebungen).

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

2. Klicken Sie auf die Schaltfläche "Importieren".

   Das Fenster "Umgebung importieren" wird angezeigt.

3. Suchen Sie nach der entsprechenden ZIP-Datei, um eine Umgebung zu importieren.
4. Klicken Sie auf "Fertig stellen".

Die Umgebung wird in CA IdentityMinder importiert.

## Neustarten einer CA IdentityMinder-Umgebung

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Environments" (Umgebungen).

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

2. Klicken Sie auf den Namen der CA IdentityMinder-Umgebung, die Sie starten möchten.

   Das Fenster "CA IdentityMinder Environment Properties" (Umgebungseigenschaften) wird angezeigt.

3. Wählen Sie eine der folgenden Optionen aus:

   **Restart Environment (Umgebung neu starten)**

   Wird verwendet, um eine Umgebung anzuhalten und zu starten.

   **Beenden**

   Hält eine Umgebung an, die gegenwärtig ausgeführt wird.

   **Starten**

   Startet eine Umgebung, die gegenwärtig nicht ausgeführt wird.

## Löschen einer CA IdentityMinder-Umgebung

Verwenden Sie diesen Vorgang, um eine CA IdentityMinder-Umgebung zu entfernen.

**Hinweis:** Wenn CA IdentityMinder mit SiteMinder für die erweiterte Authentifizierung integriert wird, löscht CA IdentityMinder auch die SiteMinder-Richtliniendomäne, die die Umgebung und die Standard-Authentifizierungsschemen schützt, die für die Umgebung erstellt werden.

**Gehen Sie wie folgt vor:**

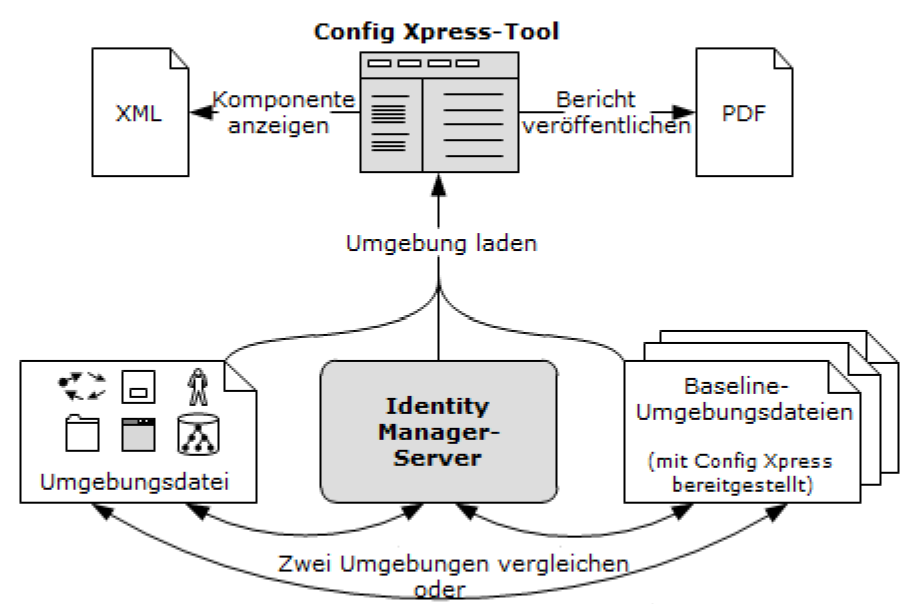
1. Aktivieren Sie im Fenster "Environments" (Umgebungen) das Kontrollkästchen für die zu löschenden CA IdentityMinder-Umgebungen.
2. Klicken Sie auf "Löschen".

   In CA IdentityMinder wird eine Bestätigungsmeldung angezeigt.
3. Klicken Sie auf "OK", um den Löschvorgang zu bestätigen.

# Verwalten von Konfigurationen

Config Xpress ist ein Tool, das mit CA IdentityMinder bereitgestellt wird. Sie können dieses Tool verwenden, um die Konfigurationen Ihrer CA IdentityMinder-Umgebungen zu analysieren und um mit diesen Konfigurationen zu arbeiten.

Vor allem können Sie mit dem Tool Komponenten zwischen Umgebungen verschieben. Config Xpress entdeckt automatisch andere erforderliche Komponenten und fordert Sie dazu auf, diese auch zu verschieben. Dies kann Ihnen Arbeit ersparen und das Risiko von Problemen reduzieren.




**Gehen Sie wie folgt vor:**

1. Richten Sie Config Xpress ein (siehe Seite 221).
2. Um das Tool verwenden zu können, laden Sie eine CA IdentityMinder-Umgebung (siehe Seite 222) in Config Xpress, um sie zu analysieren.
3. Verwenden Sie Config Xpress, um diese Aufgaben für die geladene Umgebung auszuführen:
   - Verschieben Sie Komponenten zwischen Umgebungen (siehe Seite 224).
   - Veröffentlichen Sie einen PDF-Bericht mit den Systemkomponenten (siehe Seite 225).
   - Zeigen Sie die XML-Konfiguration für eine bestimmte Komponente an (siehe Seite 226).

## Einrichten von Config Xpress

Die Installationsdateien für Config Xpress sind auf dem Installationslaufwerk enthalten, aber das Tool ist nicht installiert.

Für Config Xpress gelten die folgenden Softwarevoraussetzungen:

- CA IdentityMinder r12.0 und höher
- Windows-Betriebssystem
- Adobe Air-Laufzeitumgebung
- PDF-Reader für die Anzeige von Berichte

**Gehen Sie wie folgt vor:**

1. Laden Sie die Adobe Air-Laufzeitumgebung von http://get.adobe.com/air herunter, und installieren Sie sie.
2. Stellen Sie sicher, dass die Verwaltungstools installiert sind.
3. Suchen Sie im folgenden Verzeichnis nach der Installationsdatei für Config Xpress:

   ```
   C:\Programme\CA\Identity Manager\IAM Suite\Identity
   Manager\tools\ConfigXpress
   ```

4. Führen Sie "Config Xpress.air" aus, um Config Xpress zu installieren.
5. Wenn die Installation abgeschlossen ist, wird Config Xpress gestartet.

## Laden einer Umgebung in Config Xpress

Um Config Xpress verwenden zu können, müssen Sie mindestens eine Umgebung in das Tool laden. Diese Aufgabe ermöglicht es Ihnen, mit der Umgebung in Config Xpress zu arbeiten.

Sie können eine Umgebung direkt von einem CA IdentityMinder-Live-Server in Config Xpress laden, oder Sie können sie aus einer Umgebungsdatei laden. Wenn Sie eine der Baseline-Umgebungsdateien verwenden, die mit Config Xpress installiert werden, können Sie Ihre Umgebung mit der standardmäßigen Konfiguration vergleichen.

Das Laden einer Umgebung kann einige Minuten dauern.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie Config Xpress.
2. So laden Sie eine **Live-Umgebung** direkt von einem CA IdentityMinder-Server:
   a. Klicken Sie auf die Registerkarte "Server (Network)" (Server (Netzwerk)).
   b. Geben Sie den Namen und den Port des CA IdentityMinder-Servers ein. Beispiel:

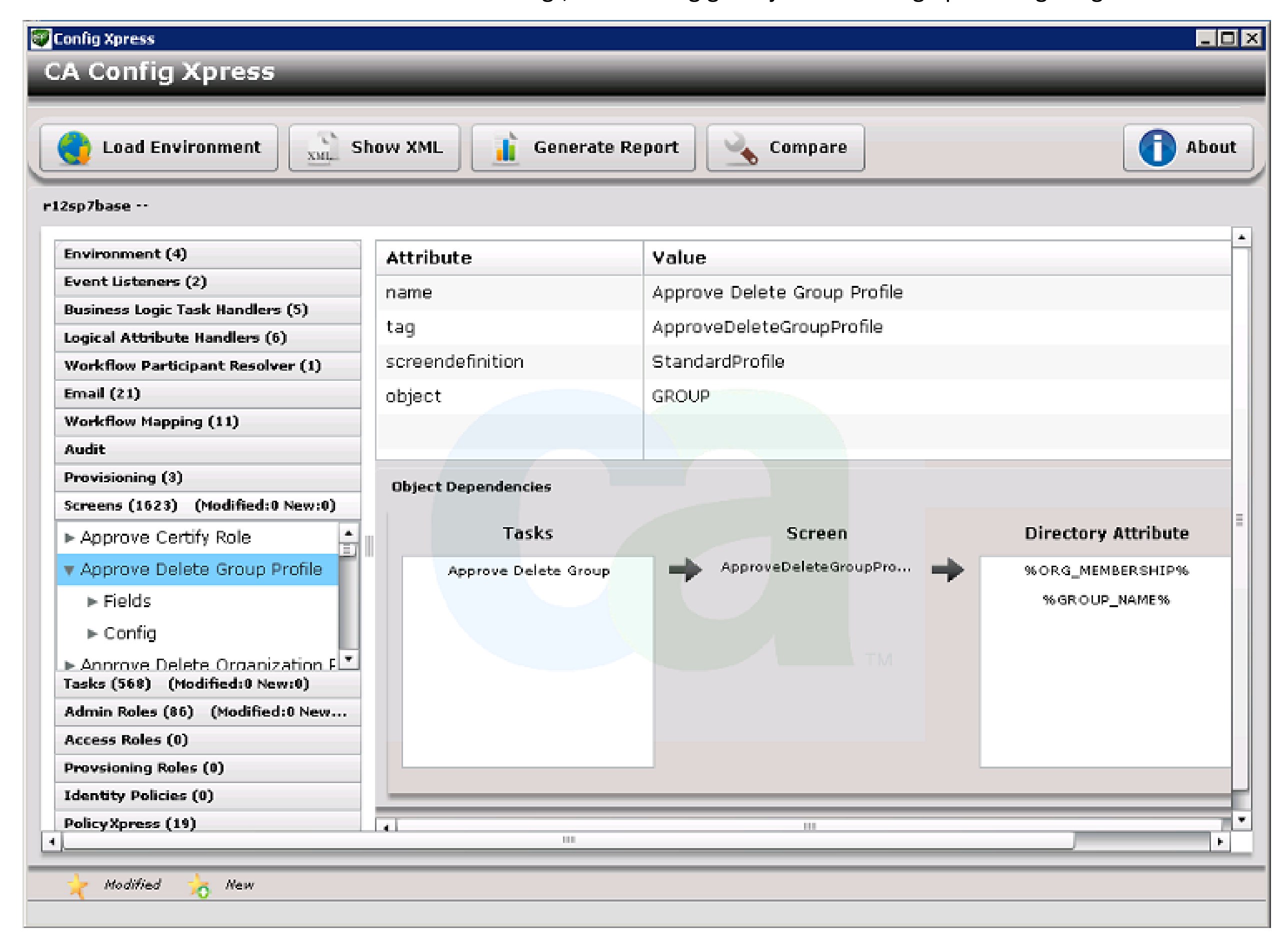
      ```
      servername.ca.com:8080
      ```
   c. Wählen Sie "HTTPS verwenden" aus, wenn Ihr Server so eingerichtet ist, dass nur HTTPS verwendet werden kann.
   d. Wählen Sie "12.5 SP7" aus, wenn der Server eine höhere Version als r12.5 SP6 hat.
   e. Klicken Sie auf "Verbinden".
   f. Wählen Sie eine Umgebung aus der Liste *Choose Environment to load* (Zu ladende Umgebung auswählen) aus, und klicken Sie dann auf "Laden".
3. So laden Sie eine **Umgebungsdatei,** die aus Ihrer CA IdentityMinder-Umgebung exportiert wurde:
   a. Exportieren Sie eine CA IdentityMinder-Umgebung.
   b. Klicken Sie in Config Xpress auf die Registerkarte "File System" (Dateisystem).
   c. Wählen Sie die Version aus, suchen Sie die Umgebungsdatei, und klicken Sie dann auf "Laden".
4. So laden Sie eine **Baseline-Umgebungsdatei**, die mit Config Xpress installiert wurde:
   a. Klicken Sie auf die Registerkarte "Base Versions" (Basisversionen).
   b. Wählen Sie die gewünschte Version aus, und klicken Sie dann auf "Auswählen".

Config Xpress analysiert die Umgebung und zeigt dann Details der Umgebung an.

Sie können jetzt einen Teil oder die gesamte Umgebung als PDF (siehe Seite 225) oder XML (siehe Seite 226) veröffentlichen. Wenn Sie eine zweite Umgebung laden, können Sie die Umgebungen vergleichen und Komponenten zwischen ihnen verschieben (siehe Seite 224).

**Beispiel: Config Xpress nach dem Laden einer Baseline-Konfigurationsdatei**

Dieser Screenshot zeigt, wie abhängige Objekte in Config Xpress angezeigt werden:



## Verschieben von Komponenten aus einer Umgebung in eine andere

Ohne Config Xpress ist das Verschieben von Komponenten zwischen Staging-Bereichen eine komplexe Aufgabe, die mit hoher Wahrscheinlichkeit fehlschlägt.

Wenn Config Xpress für das Verschieben der Komponenten verwendet wird, werden mit dem Tool auch alle erforderlichen Objekte verschoben. Wenn Sie zum Beispiel eine Aufgabe verschieben, die ein Fenster erfordert, werden Sie in Config Xpress gefragt, ob Sie auch die erforderlichen Komponenten auswählen möchten. Config Xpress weiß, dass die Aufgabe dieses Fenster verwendet und auch zur Zielumgebung verschoben werden sollte.

Wenn Sie eine Komponente in eine Live-Umgebung verschieben möchten, wird sie von Config Xpress sofort hochgeladen. Wenn Sie die Komponente in eine Umgebungsdatei verschieben möchten, speichern Sie die Komponente als XML-Datei und importieren Sie diese Datei dann in die Umgebung.

**Gehen Sie wie folgt vor:**

1. Laden Sie die Umgebung, die die Komponente enthält, die Sie verschieben möchten.
2. Vergleichen Sie diese Umgebung mit einer zweiten:
   a. Klicken Sie auf "Compare" (Vergleichen).
   b. Laden Sie die Zielumgebung.

      Config Xpress zeigt eine Liste der Unterschiede zwischen den beiden Umgebungen an.
3. Suchen Sie in der Liste mit den Unterschieden nach einer Komponente, die Sie verschieben möchten. Zum Sortieren der Liste können Sie auf die Spalte "Name" klicken.
4. Führen Sie für jede Komponente die folgenden Schritte aus:
   a. Wählen Sie das Element in der Spalte "Aktion" aus.

      Config Xpress analysiert die Komponente. Dieser Vorgang kann etwas Zeit in Anspruch nehmen.
   b. Wenn die Komponente abhängige Komponenten aufweist, wird das Feld "Add Modified Dependant Screens" (Geänderte abhängige Fenster hinzufügen) angezeigt. Klicken Sie auf "Ja" oder "Nein", um fortzufahren.

   Wenn Sie alle zu verschiebenden Komponenten ausgewählt haben, können Sie damit beginnen, die aktualisierten Komponenten zu verschieben.
5. Wenn Sie die Komponenten auf einen Live-Server verschieben, klicken Sie auf "Upload To" (Hochladen auf).

   Die Komponenten werden sofort verschoben.
6. Wenn Sie die Komponenten in eine Umgebungsdatei verschieben:

a. Klicken Sie auf "Speichern".

b. Geben Sie einen Dateinamen ein, und klicken Sie erneut auf "Speichern".

   Config Xpress speichert alle Komponenten, die Sie in einer XML-Datei ausgewählt haben. Sie können diese XML-Datei jetzt in die eigentliche Zielumgebung importieren.

## Veröffentlichen von PDF-Berichten

Config Xpress kann einen Bericht generieren, in dem der aktuelle Status einer CA IdentityMinder-Umgebung dokumentiert wird. Sie können diesen Bericht verwenden, um einen Snapshot einer Produktionsumgebung zu erstellen. Wenn Sie den Bericht generieren, wählen Sie aus, ob Sie die vollständige Konfiguration oder nur die Änderungen seit der Installation erfassen möchten.

Dieser Bericht ist als zukünftige Referenz oder als Teil eines Systemwiederherstellungsplans hilfreich.

**Gehen Sie wie folgt vor:**

1. Laden Sie eine Umgebung in Config Xpress.
2. Klicken Sie auf "Generate Report" (Bericht generieren).

   Im Dialogfeld "Generate PDF Report" (PDF-Bericht generieren) können Sie die Schriftgröße ändern und Text für den Titel oder Deckblätter eingeben. Sie können hier auch auswählen, ob Sie alle Konfigurationselemente oder nur neue bzw. geänderte Elemente einschließen möchten.

   **Wichtig!** Wenn Sie nicht auf das Feld *Only include details of new or modified tasks, screens, roles* (Nur Details zu neuen oder geänderten Aufgaben, Fenstern, Rollen einschließen) klicken, enthält der Bericht die gesamte Umgebung. Die PDF-Datei ist dann ca. 2.000 Seiten lang und über 40 MB groß.

3. Klicken Sie auf "OK".
4. Geben Sie einen Dateinamen ein, und speichern Sie den Bericht. Der Speichervorgang kann ein paar Minuten dauern - oder viel länger, wenn Sie die gesamte Umgebung veröffentlichen.

   Der Bericht wird in einem PDF-Reader geöffnet.

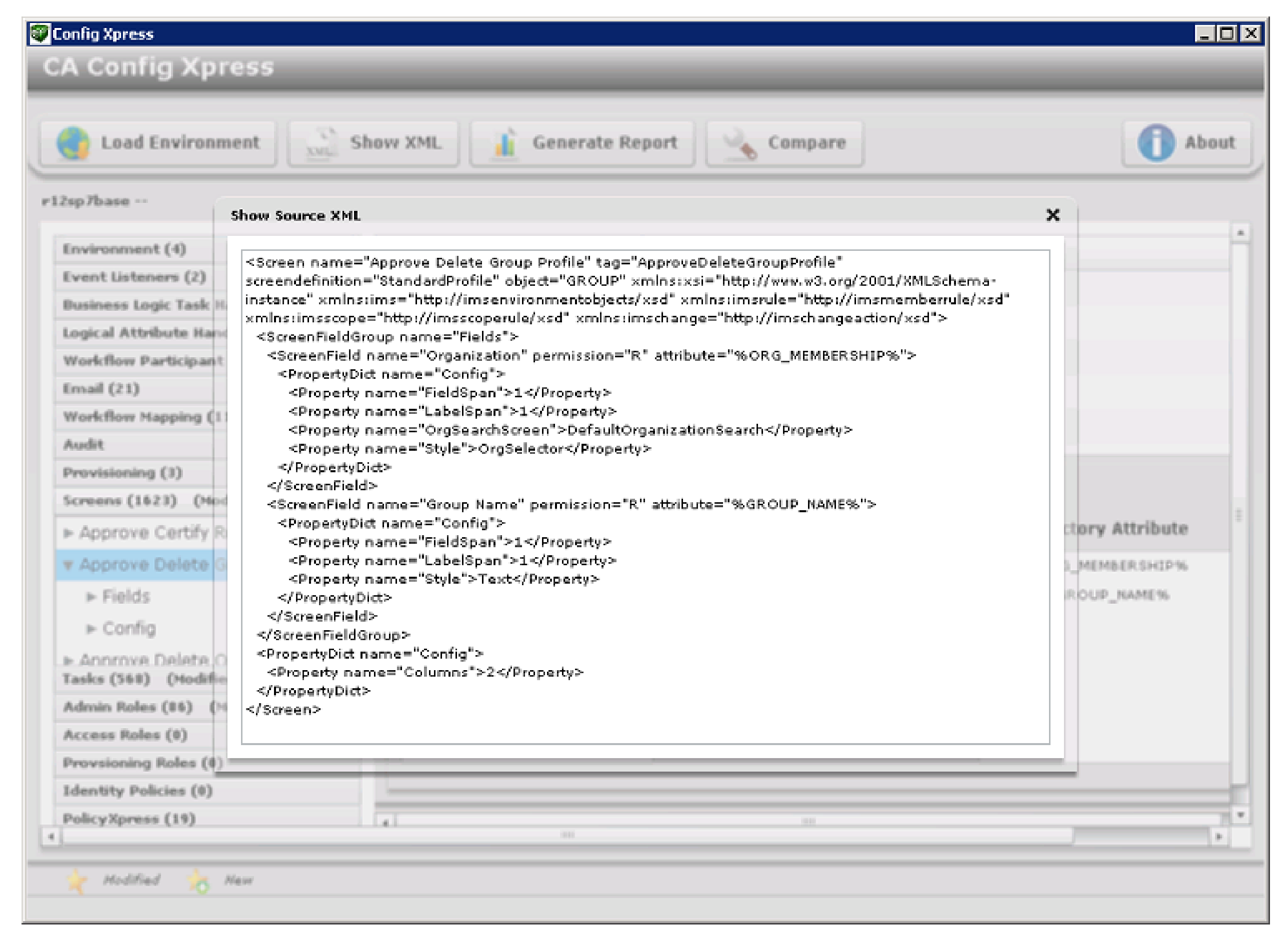
## Anzeigen der XML-Konfiguration

Config Xpress kann die XML-Konfiguration für eine bestimmte Komponente anzeigen. Die Informationen in dieser XML-Datei helfen Ihnen dabei, sich mit einem System vertraut zu machen.

**Gehen Sie wie folgt vor:**

1. Laden Sie eine Umgebung in Config Xpress.
2. Klicken Sie auf eine Komponente im Config Xpress-Fenster.
3. Klicken Sie auf "XML anzeigen".

   Die XML-Konfiguration wird angezeigt:



# Optimieren der Auswertung von Richtlinienregeln

Richtlinienregeln, die eine Gruppe von Benutzern dynamisch identifizieren, werden in der Auswertung von Richtlinien der Rollen Mitglied, Admin und Eigentümer und von Identitätsrichtlinien verwendet. Die Auswertung dieser Regeln kann in großen CA IdentityMinder-Implementierungen viel Zeit in Anspruch nehmen.

**Hinweis**: Weitere Informationen zu Mitglieds-, Admin-, Eigentümer- und Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

Sie können die Auswertungszeit für Regeln mit Benutzerattributen verkürzen, indem Sie die Option für die Auswertung im Arbeitsspeicher aktivieren. Wenn die Option für die Auswertung im Arbeitsspeicher aktiviert ist, ruft CA IdentityMinder Informationen über einen zu bewertenden Benutzer aus dem Benutzerspeicher ab und speichert eine Repräsentation dieses Benutzers im Arbeitsspeicher. CA IdentityMinder verwendet die Repräsentation im Arbeitsspeicher, um die Attributwerte in Bezug auf die Richtlinienregeln zu vergleichen. Dadurch wird die Anzahl der Aufrufe beschränkt, die CA IdentityMinder direkt im Benutzerspeicher durchführt.

Sie aktivieren die Option für die Auswertung im Arbeitsspeicher für eine Umgebung in der Management-Konsole.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die Managementkonsole.
2. Wählen Sie "Environments" (Umgebungen), *Environment Name*, (Umgebungsname), "Advanced Settings" (Erweiterte Einstellungen), "Miscellaneous" (Verschiedene) aus.

   Die Seite "User Defined Properties" (Benutzerdefinierte Eigenschaften) wird geöffnet.
3. Geben Sie den folgenden Text im Feld "Property" (Eigenschaft) ein:

   UseInMemoryEvaluation
4. Geben Sie *eine* der folgenden Zahlen im Feld "Value" (Wert) ein:

   **0**

   Die Auswertung im Arbeitsspeicher ist deaktiviert.

   **1**

   Die Auswertung im Arbeitsspeicher ist aktiviert. Wenn diese Option festgelegt ist, wird beim Attributvergleich die Groß-/Kleinschreibung berücksichtigt.

   **3**

   Die Auswertung im Arbeitsspeicher ist aktiviert. Wenn diese Option festgelegt ist, wird beim Attributvergleich die Groß-/Kleinschreibung nicht berücksichtigt.
5. Klicken Sie auf "Hinzufügen".

CA IdentityMinder fügt die neue Eigenschaft in der Liste der vorhandenen Eigenschaften für die Umgebung hinzu.

6. Klicken Sie auf "Speichern".

# Role and Task Settings (Rollen- und Aufgabeneinstellungen)

Im Fenster "Role and Task Settings" (Rollen- und Aufgabeneinstellungen) in der Management-Konsole können Sie Fenster-, Registerkarten-, Rollen- und Aufgabeneinstellungen in eine XML-Datei, die als Rollendefinitionsdatei bezeichnet wird, importieren oder aus dieser Datei exportieren. CA IdentityMinder stellt vordefinierte Rollendefinitionsdateien bereit, mit denen Fenster, Registerkarten, Rollen und Aufgaben für eine Reihe von Funktionen erstellt werden. Zum Beispiel gibt es eine Rollendefinitionsdatei, die Smart Provisioning unterstützt, und andere Dateien, die Fenster für die Endpunktverwaltung unterstützen.

Darüber hinaus können Sie eine Rollendefinitionsdatei verwenden, um die Einstellungen von einer Umgebung auf mehrere Umgebungen zu übertragen. Führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie Fenster-, Registerkarten-, Aufgaben- und Rolleneinstellungen in einer Umgebung.
- Exportieren Sie diese Einstellungen in eine XML-Datei.
- Importieren Sie die XML-Datei in die gewünschte Umgebung.

## Exportieren von Rollen- und Aufgabeneinstellungen

Gehen Sie folgendermaßen vor, um Rollen- und Aufgabeneinstellungen zu exportieren.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste von CA IdentityMinder-Umgebungen wird angezeigt.

2. Klicken Sie auf den Namen der entsprechenden CA IdentityMinder-Umgebung.

   Das Eigenschaftsfenster für diese Umgebung wird angezeigt.

3. Klicken Sie auf "Role and Task Settings" (Rollen- und Aufgaben-Einstellungen) und anschließend auf "Export".
4. Klicken Sie auf "Öffnen", um die Datei in einem Browserfenster anzuzeigen, oder auf "Speichern", um die Einstellungen in einer XML-Datei zu speichern.

## Importieren von Rollen- und Aufgabeneinstellungen

Rollen- und Aufgabeneinstellungen werden in XML-Dateien definiert, die als Rollendefinitionsdateien bezeichnet werden. Sie können vordefinierte Rollendefinitionsdateien importieren, um bestimmte CA IdentityMinder-Funktionssätze (zum Beispiel Smart Provisioning) zu unterstützen, oder Rollendefinitionsdateien in eine Umgebung aus einer anderen importieren.

**Hinweis:** Sie können auch Rollendefinitionen für benutzerdefinierte Connectors importieren, die mit Connector Xpress erstellt werden. Sie erstellen diese Rollendefinitionsdateien mit dem Generator für Rollendefinitionen. Weitere Informationen finden Sie im *Connector Xpress-Handbuch*.

Gehen Sie folgendermaßen vor, um Rollen- und Aufgabeneinstellungen zu importieren.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Managementkonsole auf "Umgebungen".

   Eine Liste von CA IdentityMinder-Umgebungen wird angezeigt.

2. Klicken Sie auf den Namen der CA IdentityMinder-Umgebung, in die Sie die Rollen- und Aufgabeneinstellungen importieren möchten.

   Das Eigenschaftsfenster für diese Umgebung wird angezeigt.

3. Klicken Sie auf "Role and Task Settings" (Rollen- und Aufgaben-Einstellungen) und anschließend auf "Importieren".

4. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie eine oder mehrere Rollendefinitionsdateien aus, um Standardrollen und -aufgaben für die Umgebung zu erstellen.

     Um alle verfügbaren Rollendefinitionsdateien auszuwählen, klicken Sie auf "Select/Deselect All" (Alle auswählen/Gesamte Auswahl aufheben).

   - Geben Sie den Pfad und Dateinamen für die zu importierende Rollendefinitionsdatei ein, oder suchen Sie nach der Datei. Klicken Sie dann auf "Fertig stellen".

5. Klicken Sie auf "Fertig stellen".

   Der Status wird im Ausgabefenster der Rollenkonfiguration angezeigt.

6. Klicken Sie zum Beenden auf "Fortfahren".

## Erstellen von Rollen und Aufgaben für dynamische Endpunkte

Mithilfe von Connector Xpress können Sie dynamische Connector konfigurieren, um die Bereitstellung und Verwaltung von SQL-Datenbanken und LDAP-Verzeichnissen zu ermöglichen. Sie können den Generator für Rollendefinitionen für jeden dynamischen Connector verwenden, um Aufgaben- und Fensterdefinitionen für Kontoverwaltungsfenster zu erstellen, die in der Benutzerkonsole angezeigt werden.

Nachdem Sie den Generator für Rollendefinitionen ausgeführt haben, importieren Sie die sich ergebende Rollendefinitionsdatei (siehe Seite 229) in die Management-Konsole.

**Hinweis:** Weitere Informationen zum Generator für Rollendefinitionen finden Sie im *Connector Xpress-Handbuch*.

# Ändern des Systemmanager-Kontos

Ein Systemmanager ist für die Einrichtung und Verwaltung von CA IdentityMinder-Umgebungen verantwortlich. Zu den typischen Aufgaben eines Systemmanagers gehören:

- Erstellen und Verwalten der anfänglichen Umgebung
- Erstellen und Ändern von Admin-Rollen
- Erstellen und Ändern von anderen Administratorkonten

Sie erstellen ein Systemmanagerkonto, wenn Sie eine CA IdentityMinder-Umgebung erstellen. Wenn dieses Konto gesperrt ist - zum Beispiel, wenn der Systemmanager das Kennwort vergessen hat -, können Sie das Konto mithilfe des Systemmanager-Assistenten erneut erstellen.

Der Systemmanager-Assistent leitet Sie schrittweise durch den Vorgang zum Zuweisen einer Systemverwaltungsrolle zu einem Benutzer.

Beachten Sie vor dem Ändern eines Systemmanagerkontos Folgendes:

- Vergewissern Sie sich, dass Sie einen LDAP-Benutzerspeicher verwenden und einen Benutzercontainer wie ou=People in der Verzeichniskonfigurationsdatei (directory.xml) für Ihr CA IdentityMinder-Verzeichnis konfiguriert haben. Die ausgewählten Benutzer müssen in dem gleichen Container vorhanden sein, in dem Sie den Systemmanager konfigurieren. Die Auswahl eines Benutzerkontos, das im Benutzercontainer nicht vorhanden ist, kann Fehler verursachen.
- Wenn die CA IdentityMinder-Umgebung ein Benutzerverzeichnis mit einer flachen Benutzerstruktur verwaltet, muss das Profil des ausgewählten Benutzers auch die Organisation einschließen. Um sicherzustellen, dass das Profil eines Benutzers richtig konfiguriert wird, fügen Sie dem physischen Attribut, das dem bekannten Attribut %ORG_MEMBERSHIP% in der directory.xml-Datei (siehe Seite 87) entspricht, den Namen der Organisation des Benutzers hinzu. Wenn zum Beispiel die Beschreibung des physischen Attributs dem bekannten Attribut %ORG_MEMBERSHIP% in der directory.xml-Datei zugeordnet ist und der Benutzer zur Organisation "Employees" gehört, muss das Profil des Benutzers das Attribut-/Wertpaar "description=Employees" enthalten.

**Gehen Sie wie folgt vor:**

1. Klicken Sie im CA IdentityMinder-Umgebungsfenster auf den Namen der entsprechenden CA IdentityMinder-Umgebung.

   Die Eigenschaften dieses spezifischen Umgebungsfensters werden angezeigt.
2. Klicken Sie auf "System Manager" (Systemmanager).

   Der Systemmanager-Assistent wird angezeigt.
3. Geben Sie den eindeutigen Namen des Benutzers mit der Systemmanager-Rolle wie folgt ein:
   - Geben Sie für Benutzer von relationalen Datenbanken die eindeutige Kennung für den Benutzer oder den Wert, der dem bekannten Attribut %USER_ID% in der Verzeichniskonfigurationsdatei zugeordnet ist, ein.
   - Geben Sie für LDAP-Benutzer den relativen DN des Benutzers ein. Wenn der DN des Benutzers zum Beispiel uid=Admin1, ou=People, ou=Employees, ou=NeteAuto lautet, geben Sie "Admin1" ein.

   **Hinweis:** Vergewissern Sie sich, dass der Systemmanager nicht *der* gleiche Benutzer wie der Administrator des Benutzerspeichers ist.
4. Klicken Sie auf "Validieren", um die vollständige Kennung des Benutzers anzuzeigen.
5. Klicken Sie auf "Weiter".

6. Wählen Sie auf der zweiten Seite des Assistenten eine Rolle aus, um sie dem Benutzer wie folgt zuzuweisen:

   - Wenn Sie die Systemmanager-Rolle zuweisen möchten, führen Sie die folgenden Aufgaben aus:

     a. Wählen Sie das Optionsfeld neben der Systemmanager-Rolle aus.

     b. Klicken Sie auf "Fertig stellen".

   - Wenn Sie eine andere Rolle als die des Systemmanagers zuweisen möchten, führen Sie die folgenden Aufgaben aus:

     a. Wählen Sie in der ersten Liste eine Bedingung aus.

     b. Geben Sie im zweiten Listenfeld den Teil eines Rollennamens oder einen vollständigen Rollennamen oder ein Sternchen (*) ein. Klicken Sie auf "Suchen".

     c. Wählen Sie die zuzuweisende Rolle aus der Suchergebnisliste aus.

     d. Klicken Sie auf "Fertig stellen".

   Im Fenster "System Manager Configuration Output" (Systemmanager-Konfigurationsausgabe) werden die Statusinformationen angezeigt.

7. Klicken Sie auf "Fortfahren", um den Systemmanager-Assistenten zu schließen.

# Aufrufen des Status einer CA IdentityMinder-Umgebung

CA IdentityMinder umfasst eine Statusseite, auf der Sie die folgenden Statusinformationen überprüfen können:

- Das CA IdentityMinder-Verzeichnis ist ordnungsgemäß geladen.
- CA IdentityMinder kann eine Verbindung mit dem Benutzerspeicher herstellen.
- Die CA IdentityMinder-Umgebung wird ordnungsgemäß geladen.

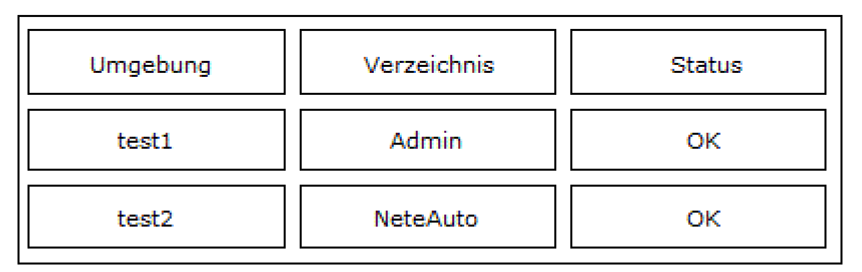
Um auf die Statusseite zuzugreifen, geben Sie die folgende URL in einem Browser ein:

`http://`*`Hostname`*`/iam/im/status.jsp`

***Hostname***

Bestimmt den vollqualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist, zum Beispiel myserver.mycompany.com.

Wenn die CA IdentityMinder-Umgebung ordnungsgemäß gestartet wird und alle Verbindungen erfolgreich hergestellt wurden, sieht die Statusseite ähnlich der folgenden Abbildung aus:



| Umgebung | Verzeichnis | Status |
| --- | --- | --- |
| test1 | Admin | OK |
| test2 | NeteAuto | OK |

Auf der Statusseite wird auch angegeben, ob die Umgebung mit FIPS 140-2 konform ist.

## Fehlerbehebung in CA IdentityMinder-Umgebungen

In der folgenden Tabelle werden mögliche Fehlermeldungen und der Fehlerbehebungsprozess beschrieben:

<table>
<tr><th>Meldung</th><th>Beschreibung</th><th>Fehlerbehebung</th></tr>
<tr><td>Nicht geladen</td><td>Das CA IdentityMinder-Verzeichnis, das der Umgebung zugeordnet ist, wurde beim Starten von CA IdentityMinder nicht geladen.</td><td rowspan="2">1. Stellen Sie sicher, dass der Benutzerspeicher ausgeführt wird.<br>Wenn CA IdentityMinder mit SiteMinder integriert ist, überprüfen Sie, ob SiteMinder eine Verbindung mit dem Benutzerspeicher herstellen kann.<br>In der Richtlinienserver-Benutzeroberfläche können Sie die Verbindung überprüfen, indem Sie die Eigenschaftsseite für die Verbindung mit dem SiteMinder-Benutzerverzeichnis öffnen, die dem Benutzerspeicher zugeordnet ist, und auf die Schaltfläche "Inhalt anzeigen" klicken.<br>Wenn der Inhalt des Benutzerspeichers angezeigt wird, kann SiteMinder die Verbindung erfolgreich herstellen.<br>Weitere Informationen zum Richtlinienserver finden Sie im CA SiteMinder Web Access Manager Policy Server-Konfigurationshandbuch.<br>2. Starten Sie CA IdentityMinder und den Richtlinienserver neu.</td></tr>
<tr><td>Not OK (Nicht OK)</td><td>CA IdentityMinder kann keine Verbindung mit dem CA IdentityMinder-Verzeichnis herstellen.</td></tr>
</table>

| Meldung | Beschreibung | Fehlerbehebung |
|---|---|---|
| SM connection is not OK (SM-Verbindung ist nicht OK) | CA IdentityMinder kann keine Verbindung mit dem SiteMinder-Richtlinienserver (für Implementierungen, einschließlich SiteMinder) herstellen | 1. Überprüfen Sie Folgendes:<br>■ Der Richtlinienserver wird ausgeführt.<br>■ Der Web-Agent schützt die Ressourcen.<br>Sie können überprüfen, ob der Web-Agent ordnungsgemäß ausgeführt wird, indem Sie auf die Richtlinienserver-Benutzeroberfläche zugreifen. Wenn eine Aufforderung angezeigt wird, die Anmeldeinformationen einzugeben, wird der Web-Agent ordnungsgemäß ausgeführt.<br>2. Starten Sie CA IdentityMinder und den Richtlinienserver neu. |
| IMS is not available now (IMS ist zu diesem Zeitpunkt nicht verfügbar) | In CA IdentityMinder ist ein Fehler aufgetreten. | Überprüfen Sie das Anwendungsserverprotokoll in Bezug auf Fehlerdetails. |
| 500-Fehlermeldung von Windows | Die Statusseite wird nicht angezeigt, wenn darauf zugegriffen wird, während die Konnektivität mit dem LDAP-Benutzerverzeichnis entfernt wird. | Deaktivieren Sie die Internetbrowser-Option "Show friendly error message" (Kurze HTTP-Fehlermeldungen anzeigen), um die Statusseite anzuzeigen. |

# Kapitel 7: Erweiterte Einstellungen

Im Fenster "Advanced Settings" (Erweiterte Einstellungen) der Management-Konsole können Sie die folgenden Aufgaben ausführen:

- Zugreifen auf Fenster zum Konfigurieren erweiterter Einstellungen
- Importieren und Exportieren erweiterter Einstellungen, wie in Importieren/Exportieren von benutzerdefinierten Einstellungen (siehe Seite 249) beschrieben

Dieses Kapitel enthält folgende Themen:

Überprüfung (siehe Seite 235)
Business Logic Task-Handler (siehe Seite 236)
Ereignisliste (siehe Seite 237)
E-Mail-Benachrichtigungen (siehe Seite 238)
Ereignis-Listener (siehe Seite 238)
Identitätsrichtlinien (siehe Seite 239)
Logical-Attribute-Handler (siehe Seite 239)
Sonstiges (siehe Seite 240)
Benachrichtigungsregeln (siehe Seite 241)
Organisationsauswahl (siehe Seite 241)
Bereitstellung (siehe Seite 242)
Benutzerkonsole (siehe Seite 245)
Webservices (siehe Seite 247)
Workflow Properties (Workflow-Eigenschaften) (siehe Seite 248)
Work Item Delegation (Arbeitselement delegieren) (siehe Seite 248)
Workflow Participant Resolvers (Workflow-Teilnehmer-Resolver) (siehe Seite 249)
Importieren/Exportieren von benutzerdefinierten Einstellungen (siehe Seite 249)
Fehler wegen unzureichendem Speicher in Java Virtual Machine (siehe Seite 250)

## Überprüfung

In Überprüfungsprotokollen werden Datensätze für die in einer CA IdentityMinder-Umgebung ausgeführten Vorgänge aufgezeichnet. Sie können die Daten in den Überprüfungsprotokollen nutzen, um die Systemaktivität zu überwachen.

CA IdentityMinder überprüft *Ereignisse*. Ein Ereignis ist ein Vorgang, der von einer CA IdentityMinder-Aufgabe generiert wird. Eine Aufgabe kann mehrere Ereignisse generieren. Zum Beispiel kann die CreateUser-Aufgabe die Ereignisse "CreateUserEvent" und "AddToGroupEvent" generieren.

Standardmäßig exportiert CA IdentityMinder alle Ereignisinformationen in die Audit-Datenbank. Um Typ und Umfang der von CA IdentityMinder aufgezeichneten Ereignisinformationen zu steuern, führen Sie die folgenden Aufgaben aus:

- Aktivieren Sie die Überprüfung für CA IdentityMinder-Admin-Aufgaben.
- Aktivieren Sie die Überprüfung für einige oder alle von Admin-Aufgaben generierten CA IdentityMinder-Ereignisse.
- Zeichnen Sie Ereignisinformationen bei verschiedenen Status auf, zum Beispiel wenn ein Ereignis abgeschlossen oder abgebrochen wird.
- Protokollieren Sie Informationen zu Attributen, die an einem Ereignis beteiligt sind. Sie können zum Beispiel Attribute protokollieren, die sich während eines ModifyUserEvent-Ereignisses ändern.
- Legen Sie die Überprüfungsebene für Ereignisse und Attribute fest.

# Business Logic Task-Handler

Ein Business Logic Task-Handler führt benutzerdefinierte Business Logic aus, bevor eine CA IdentityMinder-Aufgabe zur Verarbeitung übergeben wird. Normalerweise validiert die benutzerdefinierte Business Logic die Daten. Zum Beispiel kann ein Business Logic Task-Handler die Mitgliedschaftsbeschränkung einer Gruppe überprüfen, bevor CA IdentityMinder der Gruppe ein Mitglied hinzufügt. Wenn die Gruppenmitgliedschaftsbeschränkung erreicht wird, zeigt der Business Logic Task-Handler eine Meldung an, die den Gruppenadministrator darüber informiert, dass das neue Mitglied nicht hinzugefügt werden konnte.

Sie können die vordefinierten Business Logic Task-Handler verwenden oder benutzerdefinierte Handler mithilfe der Business Logic Task-Handler-API erstellen.

**Hinweis:** Weitere Informationen zum Erstellen benutzerdefinierter Business Logic finden Sie im *Programmierhandbuch für Java*.

Das Fenster "Business Logic Task-Handler" enthält eine Liste der vorhandenen globalen Business Logic Task-Handler. Die Liste umfasst vordefinierte Handler, die im Lieferumfang von CA IdentityMinder enthalten sind, sowie alle an Ihrem Standort definierte angepassten Handler. CA IdentityMinder führt die Handler in der Reihenfolge aus, in der sie in dieser Liste angezeigt werden.

Globale Business Logic Task-Handler können nur in Java implementiert werden.

## Automatisches Löschen von Kennwortfeldern beim Zurücksetzen des Benutzerkennworts

Sie können CA IdentityMinder so konfigurieren, dass Kennwortfeldern automatisch gelöscht werden, wenn ein zuvor eingegebener Wert eine Kennwortrichtlinie verletzt oder wenn die Werte in den Feldern "Kennwort" und "Kennwort bestätigen" nicht übereinstimmen.

**Gehen Sie wie folgt vor:**

1. Rufen Sie die Management-Konsole auf.
2. Wählen Sie die Umgebung aus, die Sie verwalten möchten, und klicken Sie dann auf "Advanced Settings".

   Die Seite für erweiterte Einstellungen wird angezeigt.
3. Klicken Sie auf "Business Logic Task Handlers" und "BlthPasswordServices".

   Die Eigenschaftsseite für den Business Logic Task-Handler wird angezeigt.
4. Legen Sie die folgende Eigenschaften fest:

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. Überprüfen Sie, dass die Einstellungen für "ConfirmPasswordHandler" wie folgt lauten:
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   Benutzer können jetzt Kennwortfelder in der Aufgabe zum Zurücksetzen des Benutzerkennworts löschen.

# Ereignisliste

Admin-Aufgaben beinhalten *Ereignisse*. Hierbei handelt es sich um Aktionen, die von CA IdentityMinder zum Abschließen von Aufgaben ausgeführt werden. Eine Aufgabe kann mehrere Ereignisse umfassen. So kann beispielsweise die Aufgabe "Benutzer erstellen" Ereignisse für das Erstellen des Benutzerprofils, das Hinzufügen des Benutzers zu einer Gruppe und das Zuweisen von Rollen beinhalten.

CA IdentityMinder überprüft Ereignisse, setzt kundenspezifische Geschäftsregeln für die Ereignisse durch und fordern die Bestätigung der Ereignisse an, falls diese Workflow-Prozessen zugeordnet sind.

Auf dieser Seite wird eine Liste der Ereignisse angezeigt, die in CA IdentityMinder verfügbar sind.

# E-Mail-Benachrichtigungen

CA IdentityMinder kann E-Mail-Benachrichtigungen senden, wenn eine Aufgabe oder ein Ereignis abgeschlossen wird oder wenn ein der Workflow-Steuerung unterliegendes Ereignis einen bestimmten Status annimmt. Zum Beispiel kann ein Genehmiger per E-Mail darüber informiert werden, dass ein Ereignis genehmigt werden muss.

Um den Inhalt von E-Mail-Benachrichtigungen anzugeben, können Sie entweder vordefinierte E-Mail-Vorlagen verwenden oder die Vorlagen an Ihre Anforderungen anpassen.

Mithilfe der Management-Konsole können Sie die folgenden Aufgaben ausführen:

- Aktivieren von E-Mail-Benachrichtigungen für eine CA IdentityMinder-Umgebung.
- Angeben der Vorlagensätze für das Erstellen von E-Mail-Nachrichten.
- Angeben der Ereignisse und Aufgaben, für die E-Mail-Benachrichtigungen gesendet werden.

# Ereignis-Listener

Eine CA IdentityMinder-Aufgabe besteht aus einer oder mehreren Aktionen, sogenannten Ereignissen, die CA IdentityMinder während der Ausführung der Aufgabe durchführt. Die Aufgabe "Benutzer erstellen" kann beispielsweise die folgenden Ereignisse umfassen:

- CreateUserEvent - Erstellt ein Benutzerprofil in einer Organisation.
- AddToGroupEvent - (Optional) Fügt den Benutzer als Mitglied einer Gruppe hinzu.
- AssignAccessRole - (Optional) Weist einem Benutzer eine Zugriffsrolle zu.

Ein *Ereignis-Listener* überwacht die Umgebung auf ein bestimmtes Ereignis, und führt dann zu einem bestimmten Zeitpunkt im Lebenszyklus eines Ereignisses benutzerdefinierte Business Logic aus. Nachdem ein neuer Benutzer in CA IdentityMinder erstellt wurde, kann beispielsweise ein Ereignis-Listener die Informationen zum Benutzer einer Datenbank in einer anderen Anwendung hinzufügen.

**Hinweis:** Weitere Informationen zum Konfigurieren von Ereignis-Listenern finden Sie im *Programmierhandbuch für Java*.

# Identitätsrichtlinien

Eine Identitätsrichtlinie wendet einen Satz von Geschäftsänderungen auf Benutzer an, die bestimmte Regeln oder Bedingungen erfüllen. Sie können Identitätsrichtlinien für die folgenden Aufgaben verwenden:

- Automatisieren bestimmter Identitätsmanagementaufgaben wie z. B. Zuweisen von Rollen und Gruppenmitgliedschaften, Zuordnen von Ressourcen oder Ändern von Attributen von Benutzerprofilen.
- Durchsetzen, dass Pflichten getrennt werden Sie können zum Beispiel eine Identitätsrichtlinie erstellen, die verhindert, dass Mitglieder der Rolle "Scheckunterzeichner" gleichzeitig die Rolle "Scheckgenehmiger" haben.
- Konformität durchsetzen. Sie können zum Beispiel Benutzer überprüfen, die einen bestimmten Titel haben und mehr als $ 100.000 verdienen.

Sie erstellen und verwalten Identitätsrichtliniensätze in der Benutzerkonsole. Weitere Informationen zu Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

Bevor Sie Identitätsrichtlinien verwenden, führen Sie in der Management-Konsole die folgenden Aufgaben aus:

- Aktivieren Sie Identitätsrichtlinien für eine CA IdentityMinder-Umgebung.
- Legen Sie die Rekursionsebene fest (optional).

# Logical-Attribute-Handler

Mithilfe von logischen Attributen in CA IdentityMinder können Sie Attribute eines Benutzerspeichers (sogenannte *physische Attribute*) in einem benutzerfreundlichen Format in den Aufgabenfenstern anzeigen. CA IdentityMinder-Administratoren verwenden Aufgabenfenster, um Funktionen in CA IdentityMinder auszuführen.

Logische Attribute sind in Benutzerspeichern nicht vorhanden. In der Regel stellen sie mindestens ein physisches Attribut dar, um die Darstellung zu vereinfachen. Das logische Attribut *date* kann beispielsweise die physischen Attribute *month*, *day* und *year* darstellen.

Logische Attribute werden durch Logical-Attribute-Handler verarbeitet. Hierbei handelt es sich um Java-Objekte, die mit der Logical-Attribute-API geschrieben werden. Wenn zum Beispiel ein Aufgabenfenster angezeigt wird, kann ein Logical-Attribute-Handler die Daten eines physischen Attributs aus dem Benutzerspeicher in logische Attributdaten konvertieren.

Sie können die vordefinierten logischen Attribute und Logical-Attribute-Handler verwenden, die in CA IdentityMinder enthalten sind, oder mit der Logical-Attribute-API neue erstellen.

**Hinweis:** Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

# Sonstiges

Benutzerdefinierte Eigenschaften, die in diesem Fenster definiert werden, beziehen sich auf die gesamte CA IdentityMinder-Umgebung. Sie werden als Namen-/Wertpaare an die init()-Methode jedes benutzerdefinierten Java-Objekts übergeben, das Sie mit den CA IdentityMinder-APIs erstellen. Ein benutzerdefiniertes Objekt kann diese Daten auf beliebige Weise entsprechend den Anforderungen der Business Logic des Objekts verwenden.

Benutzerdefinierte Eigenschaften werden auch für ein bestimmtes benutzerdefiniertes Objekt definiert. Nehmen Sie zum Beispiel an, dass die benutzerdefinierten Eigenschaften im Eigenschaftsfenster für den Ereignis-Listener "MyListener" definiert werden. Die objektspezifischen benutzerdefinierten Eigenschaften und die in den sonstigen Fenstern definierten umgebungsweiten Eigenschaften werden in einem einzelnen Aufruf an MyListener.init() übergeben.

Um eine benutzerdefinierte Eigenschaft hinzuzufügen, geben Sie einen Eigenschaftsnamen und -wert an, und klicken Sie auf "Hinzufügen".

Wenn Sie eine oder mehrere benutzerdefinierte Eigenschaften löschen möchten, aktivieren Sie das Kontrollkästchen neben jedem zu löschenden Namen-/Wertpaar, und klicken Sie auf "Löschen".

Nachdem Sie die Änderungen durchgeführt werden, klicken Sie auf "Speichern". Starten Sie den Anwendungsserver neu, damit die Änderungen wirksam werden.

**Hinweis:** Alle sonstigen Eigenschaften beachten die Groß-/Kleinschreibung. Wenn Sie also eine Eigenschaft "SelfRegistrationLogoutUrl" und eine andere Eigenschaft "selfregistrationlogouturl" definieren, werden beide Eigenschaften hinzugefügt.

# Benachrichtigungsregeln

Eine Benachrichtigungsregel kennzeichnet Benutzer, die E-Mail-Benachrichtigung erhalten. Wenn eine Aufgabe abgeschlossen wird oder ein Ereignis in einer Aufgabe einen gewissen Status annimmt, z. B. Genehmigung ausstehend, genehmigt oder abgelehnt, erhalten die Benutzer eine E-Mail-Benachrichtigung entsprechend der Benachrichtigungsregel.

**Hinweis**: Weitere Informationen zur E-Mail-Benachrichtigungsfunktion finden Sie im *Administrationshandbuch*.

CA IdentityMinder beinhaltet die folgenden vordefinierten Benachrichtigungsregeln:

**ADMIN_ADAPTER**

Sendet eine E-Mail-Nachricht an den Administrator, der die Aufgabe initiiert hat.

**USER_ADAPTER**

Sendet eine E-Mail-Nachricht an den Benutzer, der von der Aufgabe betroffen ist.

**USER_MANAGER**

Sendet eine E-Mail-Nachricht an den Manager des Benutzers im aktuellen Kontext.

Verwenden Sie zum Erstellen benutzerdefinierter Benachrichtigungsregeln die Benachrichtigungsregel-API.

**Hinweis:** Weitere Informationen zu Benachrichtigungsregeln finden Sie im *Programmierhandbuch für Java*.

# Organisationsauswahl

Eine Organisationsauswahl ist ein benutzerdefinierter Logical-Attribute-Handler, der basierend auf den vom Benutzer während der Registrierung eingegebenen Informationen bestimmt, wo CA IdentityMinder das Profil eines selbst registrierten Benutzers erstellt. Zum Beispiel kann das Profil von Benutzern, die bei der Registrierung einen Werbungscode eingeben, einer Organisation namens "Promotional Users" hinzugefügt werden.

# Bereitstellung

Verwenden Sie dieses Fenster, wenn Sie CA IdentityMinder mit Bereitstellung nutzen.

**Hinweis:** Eine ausführliche Anleitung finden Sie unter Konfigurieren einer Umgebung für die Bereitstellung (siehe Seite 199).

Die Optionen für Bereitstellungseigenschaften lauten wie folgt:

**Aktiviert**

Gibt die Verwendung von zwei Benutzerspeichern an, einer für CA IdentityMinder und ein separater Benutzerspeicher (Bereitstellungsverzeichnis genannt) für Bereitstellungskonten. Ist diese Option deaktiviert, wird nur der CA IdentityMinder-Benutzerspeicher verwendet.

**Use Session Pool (Sitzungspool verwenden)**

Aktiviert die Verwendung eines Sitzungspools.

**Session Pool Initial Sessions (Anfängliche Sitzungen im Sitzungspool)**

Definiert die Mindestanzahl von Sitzungen, die zu Beginn im Pool verfügbar sind.

**Standardeinstellung:** 8

**Session Pool Maximum Sessions (Maximale Sitzungen im Sitzungspool)**

Definiert die Höchstanzahl von Sitzungen im Pool.

**Standardeinstellung:** 32

**Enable Password Changes from Endpoint Accounts (Kennwortänderungen auf Endpunktkonten aktivieren)**

Definiert, ob der Agent für die Kennwortsynchronisierung für jeden Benutzer im Bereitstellungsserver aktiviert wird. Diese Option ermöglicht die Kennwortsynchronisierung zwischen CA IdentityMinder-Benutzern und zugeordneten Endpunktkonten.

**Enable Accumulation of Provisioning Role Membership Events (Ansammlung von Bereitstellungsrollen-Mitgliedschaft ermöglichen)**

Wenn Sie dieses Kontrollkästchen aktivieren, führt CA IdentityMinder Ereignisse im Zusammenhang mit der Bereitstellungsrollen-Mitgliedschaft in einer bestimmten Reihenfolge aus. Alle Hinzufügungsaktionen werden zu einem einzelnen Vorgang zusammengefasst und zur Verarbeitung an den Bereitstellungsserver gesendet. Im Anschluss an die Verarbeitung dieser Hinzufügungsaktionen kombiniert CA IdentityMinder die Entfenrungsaktionen zu einem einzelnen Vorgang und sendet diesen ebenfalls an den Bereitstellungsserver. Ein einzelnes Ereignis namens "AccumulatedProvisioningRoleEvent" wird generiert, um die Ereignisse in dieser Reihenfolge auszuführen.

**Hinweis**: Weitere Informationen zu "AccumulatedProvisioningRoleEvent" finden Sie im *Administrationshandbuch*.

**Organization for Creating Inbound Users (Organisation zum Erstellen von Inbound-Benutzern)**

Definiert den vollständig qualifizierten Pfad zu dem Benutzerspeicher, den CA IdentityMinder verwendet. Dieses Feld wird nur angezeigt, wenn der Benutzerspeicher eine Organisation enthält.

**Innenadministrator**

Definiert ein CA IdentityMinder-Administratorkonto, mit dem Aufgaben im Zusammenhang mit eingehenden Zuordnungen ausgeführt werden. Diese Aufgaben sind in die Rolle "Manager für Bereitstellungssynchronisierung" eingeschlossen. Der Administrator muss in der Lage, jede Aufgabe für jeden CA IdentityMinder-Benutzer auszuführen.

## Bereitstellungsverzeichnis

Das Bereitstellungsverzeichnis ist ein Repository für Bereitstellungsinformationen, einschließlich Domäne, globaler Benutzer, Endpunkttypen, Endpunkten, Konten und Kontovorlagen. Wenn Sie es auswählen, werden weitere Optionen zum Zuordnen des CA IdentityMinder-Benutzerspeichers zum Bereitstellungsverzeichnis angezeigt.

## Ermöglichen der Erstellung von Sitzungspools

Zur Leistungssteigerung kann CA IdentityMinder bei der Kommunikation mit dem Bereitstellungsserver eine Reihe von Sitzungen für Sitzungspools vorab zuordnen.

Ist die Option für Sitzungspools deaktiviert, erstellt und löscht CA IdentityMinder Sitzungen nach Bedarf.

Für eine neue Umgebung werden Sitzungspools standardmäßig aktiviert. Für vorhandene Umgebungen können Sie Sitzungspools aktivieren.

**Gehen Sie wie folgt vor:**

1. Wählen Sie in der Management-Konsole "Advanced Settings" (Erweiterte Einstellungen) und "Provisioning" (Bereitstellung) aus.
2. Wählen Sie "Use Session Pool" (Sitzungspool verwenden) aus.
3. Definieren Sie die Mindestanzahl von Sitzungen im Pool bei der Erstellung.
4. Definieren Sie die Höchstanzahl von Sitzungen im Pool.
5. Klicken Sie auf "Speichern".
6. Starten Sie den Anwendungsserver neu.

   Der Sitzungspool wird entsprechend den definierten Einstellungen aktiviert.

## Ermöglichen der Kennwortsynchronisierung

Der Bereitstellungsserver ermöglicht die Kennwortsynchronisierung zwischen CA IdentityMinder-Benutzern und zugeordneten Endpunktbenutzerkonten. Wenn also ein Benutzer, der Bereitstellungsrollen hat, in CA IdentityMinder erstellt oder geändert wird, wird der Bereitstellungsbenutzer so eingerichtet, dass er Kennwortänderungen von Endpunktkonten zulässt.

**Hinweis:** Wenn Sie diese Funktion in der Management-Konsole aktivieren, lassen *alle* Benutzer in der Umgebung Kennwortänderungen von Endpunktkonten zu.

**So aktivieren Sie die Kennwortsynchronisierung**

1. Wählen Sie in der Management-Konsole "Advanced Settings" (Erweiterte Einstellungen) und "Provisioning" (Bereitstellung) aus.
2. Aktivieren Sie "Enable Password Changes from Endpoint Accounts" (Kennwortänderungen auf Endpunktkonten aktivieren).
3. Klicken Sie auf "Speichern".
4. Starten Sie den Anwendungsserver neu.

## Zuordnungen von Attributen

Attributzuordnungen ordnen die Benutzerattribute in mit der Bereitstellung verknüpften Admin-Aufgaben, wie "Bereitstellung: Benutzer erstellen", den entsprechenden Attributen im Bereitstellungsserver zu. Ein einzelnes Bereitstellungsattribut kann mehreren Attributen im CA IdentityMinder-Benutzerspeicher zugeordnet werden.

Für die Attribute in den Standardaufgaben sind Standardzuordnungen vorhanden, die im Abschnitt für eingehende Zuordnungen aufgeführt sind. Wenn Sie eine dieser Admin-Aufgaben ändern, sodass diese andere Attribute verwendet, müssen Sie ggf. die Attributzuordnungen aktualisieren.

## Eingehende Zuordnungen

Eingehende Zuordnungen ordnen Ereignisse, die vom Bereitstellungsserver generiert werden, einer Admin-Aufgabe zu. Diese Zuordnungen sind voreingestellt und können nicht geändert werden.

## Ausgehende Zuordnungen

Ausgehende Zuordnungen ordnen Ereignisse, die von Admin-Aufgaben generiert werden, Ereignissen zu, die auf das Bereitstellungsverzeichnis angewandt werden. Für Ereignisse, die sich auf Benutzerattribute auswirken, sind Standardzuordnungen vorhanden.

# Benutzerkonsole

Auf eine CA IdentityMinder-Umgebung wird mithilfe der Benutzerkonsole zugegriffen. Dies ist eine Webanwendung, die es Benutzern ermöglicht, Admin-Aufgaben auszuführen. Sie definieren gewisse Eigenschaften für die Benutzerkonsole, die Administratoren für den Zugriff auf die Umgebung verwenden, auf der Seite "User Console" in der Management-Konsole.

Die Seite "User Console" enthält die folgenden Felder:

**General Properties (Allgemeine Eigenschaften)**

Definieren Sie allgemeine Eigenschaften, die auf eine Umgebung angewandt werden.

**Show Recently Completed Tasks (Vor Kurzem abgeschlossene Aufgaben anzeigen)**

Bestimmt, ob CA IdentityMinder eine Statusmeldung anzeigt, wenn eine Aufgabe abgeschlossen wird.

Bei Auswahl dieser Option müssen Benutzer auf "OK" klicken, um die von CA IdentityMinder angezeigte Statusmeldung auszublenden.

Deaktivieren Sie diese Option, um die Meldung auszuschalten, sodass Benutzer beim Anzeigen einer Statusmeldung nicht immer auf "OK" klicken müssen.

**Show About Link (Link zu weiteren Informationen anzeigen)**

Bestimmt, ob in der linken unteren Ecke der Benutzerkonsole ein Link zu weiteren Informationen angezeigt wird. Bei Auswahl dieser Option können CA IdentityMinder-Benutzer über den Link "Info" Versionsinformationen zu CA IdentityMinder-Komponenten anzeigen.

**Enable Language Switching (Umschalten zwischen Sprachen aktivieren)**

Bestimmt, ob CA IdentityMinder im Anmeldefenster und in der Benutzerkonsole eine Dropdown-Liste zur Sprachenauswahl anzeigt. Bei Auswahl dieses Feldes können CA IdentityMinder-Benutzer die Sprache in der Benutzerkonsole ändern, indem sie eine neue Sprache aus der Liste auswählen.

**Hinweis:** Um das Feld für die Sprachauswahl anzuzeigen, müssen das Feld "Enable Language Switching" ausgewählt *und* CA IdentityMinder für die Unterstützung mehrerer Sprachen konfiguriert sein.

Weitere Informationen hierzu finden Sie im *User Console Design Guide*.

**Job Timeout (Job-Zeitlimit)**

Bestimmt, wie lange CA IdentityMinder nach dem Übermitteln einer Aufgabe wartet, bevor eine Statusmeldung angezeigt wird.

Wenn die Aufgabe innerhalb des angegebenen Zeitraums abgeschlossen wird, zeigt CA IdentityMinder die folgende Meldung an:

"Aufgabe abgeschlossen"

Wenn die Ausführung der Aufgabe länger dauert oder sich die Aufgabe unter Workflow-Steuerung befindet, zeigt CA IdentityMinder die folgende Meldung an:

"Task has been submitted for processing on the *current date*"

**Hinweis:** Änderungen sind möglicherweise nicht sofort wirksam.

**Theme Properties (Themeneigenschaften)**

Ermöglicht Ihnen, das Symbol und den Titel der Benutzerkonsole in einer Umgebung anzupassen. Sie können zum Beispiel den Fenstern der Benutzerkonsole ein Unternehmenslogo und den Unternehmensnamen hinzufügen.

Themeneigenschaften umfassen die folgenden Einstellungen:

**Icon (URI) (Symbol (URI))**

Definiert das Symbol mithilfe eines URI zu einem Bild auf dem Anwendungsserver.

**Beispiel:** http://myserver.mycompany.com/images/front/logo.gif

**Icon Link (URI) (Symbol-Link (URI))**

Definiert die Navigationsverknüpfung zu dem Bild mithilfe eines URI.

**Icon Title (Symboltitel)**

Definiert die QuickInfo, die beim Bewegen der Maus über das Symbol als Text angezeigt wird.

**Titel**

Gibt benutzerdefinierten Text an, der neben dem Symbol oben in der Benutzerkonsole angezeigt wird.

**Hinweis:** Wenn Sie ein benutzerdefiniertes Design definierten haben, können Sie ein Symbol oder einen Titel angeben, indem Sie auf eine Eigenschaftsdatei für das Design verweisen. Wenn zum Beispiel der Eintrag für das Symbolbild in der Eigenschaftsdatei für ein benutzerdefiniertes Design "image/logo.gif" lautet, können Sie die gleiche Zeichenfolge in das Symbolfeld eingeben.

**Login Properties (Anmeldeeigenschaften)**

Geben Sie die Authentifizierungsmethode und den Speicherort der Anmeldungsseite an, zu der Benutzer umgeleitet werden, wenn sie auf eine Umgebung zugreifen.

**Authentication Provider module class name (Klassenname des Authentifizierungsanbietermoduls)**

Gibt den Klassennamen des Authentifizierungsanbietermoduls an.

**Anmeldungsseite**

Gibt die Seite an, zu der Benutzer umgeleitet werden, wenn sie auf eine Umgebung zugreifen.

# Webservices

Der Webservice zur externen Ansteuerung von Aufgaben (Task Execution Web Service, TEWS) von CA IdentityMinder ermöglicht Clientanwendungen von Drittanbietern, CA IdentityMinder-Aufgaben zur entfernten Ausführung an CA IdentityMinder zu übermitteln.

Im Eigenschaftsfenster für Webservices können Sie den TEWS für eine Umgebung konfigurieren. In diesem Fenster können Sie die folgenden Aufgaben ausführen:

- Aktivieren Sie TEWS für eine CA IdentityMinder-Umgebung.
- Generieren Sie aufgabenspezifische WSDL-Dokumente (Web Services Definition Language).
- Lassen Sie Identitätswechsel zu.
- Geben Sie an, dass das Admin-Kennwort zur Authentifizierung erforderlich ist.
- Konfigurieren Sie die SiteMinder-Authentifizierung.
- Konfigurieren Sie SiteMinder so, dass die URL des Webservices gesichert wird, wenn CA IdentityMinder mit SiteMinder integriert ist.
- Geben Sie die Authentifizierung des Benutzernamens für Websicherheitsservices mithilfe eines Tokens an.
- Geben Sie mindestens einen der drei möglichen Authentifizierungstypen an.

Weitere Informationen zum Ausgeben von Remoteanfragen bei CA IdentityMinder durch den Webservice zur externen Ansteuerung von Aufgaben finden Sie im *Programmierhandbuch für Java*.

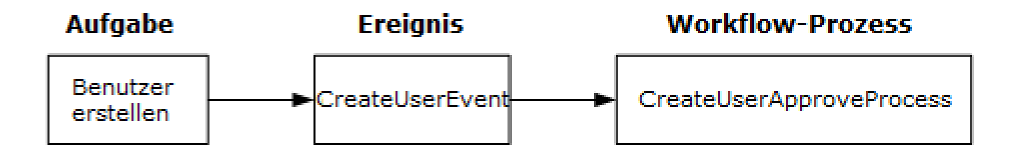
# Workflow Properties (Workflow-Eigenschaften)

Bei Aktivierung steuert die Workflow-Funktion die Ausführung einer CA IdentityMinder-Aufgabe, die einem Workflow-Vorgang zugeordnet ist.

Ein Workflow-Vorgang ist ein Satz von Schritten, die zur Erfüllung eines Geschäftsziels ausgeführt werden, z. B. zum Erstellen eines Benutzerkontos. Normalerweise beinhaltet einer dieser Schritte, dass die Aufgabe genehmigt oder zurückgewiesen wird.

Eine Admin-Aufgabe ist einem oder mehreren Ereignissen zugeordnet, die einen oder mehrere Workflow-Vorgänge auslösen können. Nachdem die Workflow-Vorgänge abgeschlossen wurden, führt CA IdentityMinder die Aufgabe aus oder weist sie zurück, je nach Ergebnis der Workflow-Vorgänge.

Die folgende Abbildung zeigt die Beziehung zwischen einer CA IdentityMinder-Aufgabe, einem zugeordneten Ereignis und einem Workflow-Vorgang:




**Workflow Properties (Workflow-Eigenschaften)**

Verwenden Sie das Kontrollkästchen, um den Workflow für die CA IdentityMinder-Umgebung zu aktivieren oder zu deaktivieren.

# Work Item Delegation (Arbeitselement delegieren)

Bei Aktivierung kann ein Teilnehmer (der Delegierer) angeben, dass einem anderen Benutzer (der Delegierte) die Berechtigung erteilt wird, Aufgaben in der Arbeitsliste des Delegierers zu genehmigen. Während der Abwesenheit des Delegierers kann der Teilnehmer einem anderen Genehmiger Arbeitselemente zuweisen. Der Delegierer behält während des Delegationszeitraums vollen Zugriff auf seine Arbeitselemente.

Zur Delegation wird das folgende bekannte Attribut verwendet:

%DELEGATORS%

Dieses bekannte Attribut speichert die Namen der Benutzer, die Arbeitselemente an den Benutzer mit dem Attribut delegieren, sowie den Zeitpunkt, zu dem die Delegation erstellt wird.

**Hinweis**: Weitere Informationen zum Delegieren von Arbeitselementen finden Sie im *Administrationshandbuch*.

# Workflow Participant Resolvers (Workflow-Teilnehmer-Resolver)

Die Aktivitäten in einem Workflow-Vorgang, wie das Genehmigen oder Zurückweisen einer Aufgabe, werden von *Teilnehmern* ausgeführt.

Im Fenster "Workflow Participant Resolvers" können Sie einer benutzerdefinierten Teilnehmerauflösung einer Java-Klasse für eine vollständig qualifizierte Teilnehmerauflösung zuordnen.

Eine benutzerdefinierte *Teilnehmerauflösung* ist ein Java-Objekt, das Teilnehmer einer Workflow-Aktivität bestimmt und eine Liste an CA IdentityMinder zurückgibt. CA IdentityMinder übergibt die Liste dann an die Workflow-Engine.

Normalerweise erstellen Sie nur dann eine benutzerdefinierte Teilnehmerauflösung, wenn keine der Standardteilnehmerauflösungen die Teilnehmerliste liefern kann, die für die Aktivität erforderlich ist.

**Hinweis:** Weitere Informationen zum Erstellen benutzerdefinierter Teilnehmerauflösungen finden Sie im *Programmierhandbuch für Java*. Weitere Informationen zu den standardmäßige Teilnehmerauflösungen finden Sie im *Administrationshandbuch*.

# Importieren/Exportieren von benutzerdefinierten Einstellungen

Im Fenster "Advanced Settings" der Management-Konsole können Sie wie folgt erweiterte Einstellungen auf mehrere Umgebungen anwenden:

- Konfigurieren Sie erweiterte Einstellungen in einer Umgebung.
- Exportieren Sie die erweiterten Einstellungen in eine XML-Datei.
- Importieren Sie die XML-Datei in die erforderlichen Umgebungen.

# Fehler wegen unzureichendem Speicher in Java Virtual Machine

**Symptom:**

In Zeiten hoher Belastung oder hoher Last werden Fehler wegen unzureichendem Speicher in JVM ausgegeben, die sich auf die Funktionalität des CA IdentityMinder-Servers auswirken.

**Lösung:**

Wir empfehlen, die JVM-Debugoptionen so festzulegen, dass bei unzureichendem Speicher eine Warnung angezeigt wird.

**Hinweis:** Weitere Informationen zum Festlegen von JVM-Debugoptionen finden Sie im Abschnitt zu Debugoptionen unter "Java HotSpot VM Options" auf http://www.oracle.com.

# Kapitel 8: Überprüfung

Dieses Kapitel enthält folgende Themen:

So konfigurieren und generieren Sie Audit-Datenberichte (siehe Seite 251)
Bereinigen der Audit-Datenbank (siehe Seite 264)

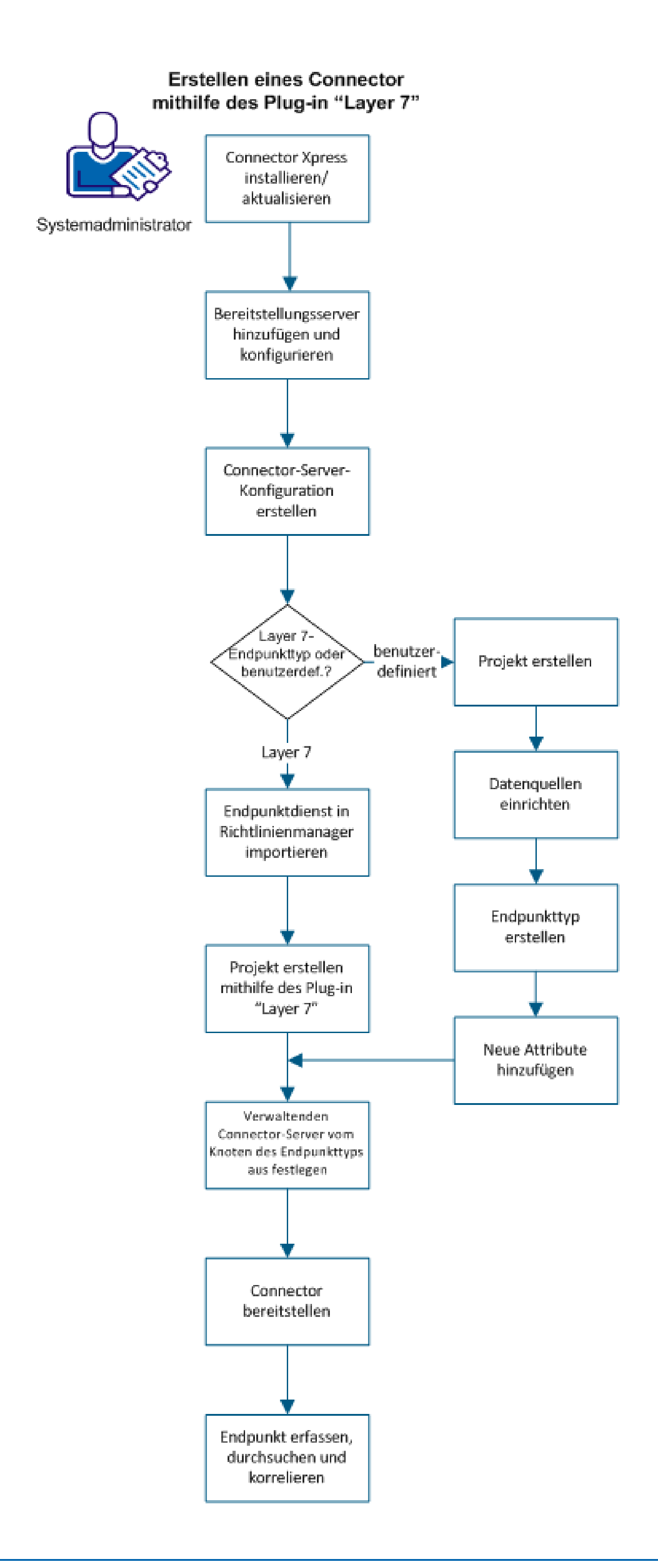
## So konfigurieren und generieren Sie Audit-Datenberichte

Audit-Daten stellen einen Verlaufsdatensatz der Vorgänge bereit, die in einer Umgebung stattfinden. Wenn Sie Überwachung konfigurieren und aktivieren, zeichnet das System Informationen zu den Aufgaben in einer Überwachungsdatenbank auf. Die Überprüfungsinformationen können zum Generieren von Berichten verwendet werden. Audit-Daten können beispielsweise Folgendes enthalten:

- Systemaktivität für einen angegebenen Zeitraum.
- Benutzeranmeldungen und -abmeldungen beim Zugriff auf eine bestimmte Umgebung.
- Die Aufgaben, die ein bestimmter Benutzer ausführt.
- Eine Liste von Objekten, die während eines bestimmten Zeitraums geändert wurden.
- Die einem Benutzer zugewiesenen Rollen.
- Die Vorgänge, die für ein bestimmtes Benutzerkonto durchgeführt werden.

Audit-Daten werden für *Ereignisse* in CA IdentityMinder generiert. Ein Ereignis ist ein Vorgang, der von einer CA IdentityMinder-Aufgabe generiert wird. So kann beispielsweise die Aufgabe "Benutzer erstellen" das Ereignis "AssignAccessRoleEvent" enthalten.

Folgendes Diagramm beschreibt, wie ein Systemadministrator die Überwachung konfiguriert und einen Bericht der Audit-Daten generiert:


Erstellen eines Connector mithilfe des Plug-in "Layer 7"
Systemadministrator
Connector Xpress installieren/ aktualisieren
Bereitstellungsserver hinzufügen und konfigurieren
Connector-Server-Konfiguration erstellen
Layer 7-Endpunkttyp oder benutzerdef.?
benutzer-definiert
Projekt erstellen
Layer 7
Datenquellen einrichten
Endpunktdienst in Richtlinienmanager importieren
Endpunkttyp erstellen
Projekt erstellen mithilfe des Plug-in "Layer 7"
Neue Attribute hinzufügen
Verwaltenden Connector-Server vom Knoten des Endpunkttyps aus festlegen
Connector bereitstellen
Endpunkt erfassen, durchsuchen und korrelieren

Stellen Sie als Administrator folgende Schritte fertig:

1. Überprüfen der Voraussetzungen (siehe Seite 254)
2. Ändern der Auditeinstellungsdatei (siehe Seite 254)
3. Aktivieren der Überwachung für eine Aufgabe (siehe Seite 259)
4. Bericht anfordern (siehe Seite 260)
5. Anzeigen des Berichts (siehe Seite 263)

## Überprüfen der Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt werden, bevor Sie Auditeinstellungen konfigurieren:

- Eine separate Datenbankinstanz wird für Speicherungsdaten erstellt, die sich auf Überwachung bezieht. Standardmäßig befindet sich die CA IdentityMinder-Datenbankschemadatei im folgenden Speicherort:
  - **Windows**: C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\Identity Manager\tools\db
- Konfigurieren Sie den Berichtsserververbindung, um den Audit-Bericht anzufordern und anzuzeigen.
- Fügen Sie ein Verbindungsobjekt für den Audit-Bericht hinzu. Führen Sie folgende Schritte aus:
  a. Melden Sie sich bei der Benutzerkonsole mit Administratorrechten an.
  b. Gehen Sie zu "Rollen und Aufgaben", "Admin-Aufgaben", und suchen Sie nach einem Audit-Bericht, der geändert werden soll.
  c. Geben Sie folgenden Verbindungsnamen im Verbindungsobjekt für das Feld "Bericht" ein:
     `rptParamConn`

## Ändern der Auditeinstellungsdatei

Konfigurieren Sie Auditeinstellungen in der Auditeinstellungsdatei, um den Informationstyp zu definieren, den CA IdentityMinder überwachen muss. Sie können eine Auditeinstellungsdatei konfigurieren, um folgende Aufgaben auszuführen:

- Überwachen Sie einige oder alle Ereignisse, die von Admin-Aufgaben generiert wurden.

- Zeichnen Sie Ereignisinformationen bei verschiedenen Status auf, zum Beispiel wenn ein Ereignis abgeschlossen oder abgebrochen wird.
- Protokollieren Sie Informationen zu Attributen, die an einem Ereignis beteiligt sind. Sie können zum Beispiel Attribute protokollieren, die sich während eines ModifyUserEvent-Ereignisses ändern.
- Legen Sie die Auditebene für die Attributprotokollierung fest.

Die Auditeinstellungsdatei ist eine XML-Datei, die Sie durch das Exportieren von Auditeinstellungen erstellen. Die Datei hat das folgende Schema:

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Weitere Informationen zu Audit-Elementen und Audit-Schema finden Sie in den Kommentaren in der Auditeinstellungsdatei.

Die AuditProfileAttribute-Elemente geben die Attribute an, die CA IdentityMinder überprüft. Die Attribute beziehen sich auf das im AuditProfile-Element angegebene Objekt.

**Hinweis:** Wenn keine Auditprofilattribute angegeben wurden, werden alle Attribute für das im AuditProfile-Element angegebene Objekt protokolliert.

Die folgende Tabelle enthält die gültigen Attribute für CA IdentityMinder-Objekttypen:

**Gültige Attribute für CA IdentityMinder-Objekttypen**

| Objekttyp | Gültige Attribute |
|---|---|
| ACCESS ROLE | ■ name - Für Benutzer sichtbarer Name der Rolle.<br>■ description - Ein optionaler Kommentar über den Zweck der Rolle.<br>■ members - Die Benutzer, die die Rolle verwenden können.<br>■ administrators - Die Benutzer, die Rollenmitglieder oder Administratoren zuweisen können.<br>■ owners - Die Benutzer, die die Rolle ändern können.<br>■ enabled - Gibt an, ob die Rolle aktiviert ist oder nicht.<br>■ assignable - Gibt an, ob die Rolle von einem Administrator zugewiesen werden kann oder nicht.<br>■ tasks - Die Zugriffsaufgaben, die der Rolle zugeordnet sind. |

**Gültige Attribute für CA IdentityMinder-Objekttypen**

| Objekttyp | Gültige Attribute |
|---|---|
| ACCESS TASK | ■ name - Für Benutzer sichtbarer Name der Aufgabe.<br>■ description - Ein optionaler Kommentar über den Zweck der Aufgabe.<br>■ application - Die Anwendung, die der Aufgabe zugeordnet ist.<br>■ tag - Die eindeutige Kennung der Aufgabe.<br>■ reserved1, reserved2, reserved3, reserved4 - Die Werte für die reservierten Felder der Aufgabe. |
| ADMINISTRATIVE ROLE | ■ name - Für Benutzer sichtbarer Name der Rolle.<br>■ description - Ein optionaler Kommentar über den Zweck der Rolle.<br>■ members - Die Benutzer, die die Rolle verwenden können.<br>■ administrators - Die Benutzer, die Rollenmitglieder oder Administratoren zuweisen können.<br>■ owners - Die Benutzer, die die Rolle ändern können.<br>■ enabled - Gibt an, ob die Rolle aktiviert ist oder nicht.<br>■ assignable - Gibt an, ob die Rolle von einem Administrator zugewiesen werden kann oder nicht.<br>■ tasks - Die Aufgaben, die der Rolle zugeordnet sind. |

| **Gültige Attribute für CA IdentityMinder-Objekttypen** | |
|---|---|
| **Objekttyp** | **Gültige Attribute** |
| ADMINISTRATIVE TASK | ■ name - Für Benutzer sichtbarer Name der Aufgabe.<br>■ description - Ein optionaler Kommentar über den Zweck der Aufgabe.<br>■ tag - Die eindeutige Kennung der Aufgabe.<br>■ category - Die Kategorie in der CA IdentityMinder-Benutzeroberfläche, unter der die Aufgabe angezeigt wird.<br>■ primary_object - Das Objekt, auf das die Aufgabe angewandt wird.<br>■ action - Der Vorgang, der für das Objekt ausgeführt wird.<br>■ hidden - Gibt an, dass die Aufgabe *nicht* in Menüs angezeigt wird.<br>■ public - Gibt an, ob die Aufgabe für Benutzer verfügbar ist, die nicht bei CA IdentityMinder angemeldet sind.<br>■ auditing - Gibt an, ob die Aufgabe die Aufzeichnung von Auditinformationen ermöglicht.<br>■ external - Gibt an, ob die Aufgabe eine externe Aufgabe ist.<br>■ url - Der URL, an den CA IdentityMinder den Benutzer umleitet, wenn eine externe Aufgabe ausgeführt wird.<br>■ workflow - Gibt an, ob die der Aufgabe zugeordneten CA IdentityMinder-Ereignisse einen Workflow auslösen.<br>■ webservice - Gibt an, ob es sich um eine Aufgabe handelt, für die über die CA IdentityMinder-Management-Konsole eine WSDL-Ausgabe (Web Services Description Language) generiert werden kann. |
| GROUP | Ein gültiges Attribut, das für das GROUP-Objekt in der Verzeichniskonfigurationsdatei (directory.xml) definiert wird. |
| ORGANIZATION<br>PARENTORG | Ein gültiges Attribut, das für das ORGANIZATION-Objekt in der Verzeichniskonfigurationsdatei (directory.xml) definiert wird. |

**Gültige Attribute für CA IdentityMinder-Objekttypen**

| Objekttyp | Gültige Attribute |
|---|---|
| RELATIONSHIP | ■ %CONTAINER% - Eindeutige Kennung des übergeordneten Objekts.<br>Wenn zum Beispiel das RELATIONSHIP-Objekt eine Rollenmitgliedschaft beschreibt, wäre der Container die Rolle.<br>■ %CONTAINER_NAME% - Für den Benutzer sichtbarer Name der übergeordneten Gruppe.<br>■ %ITEM% - Eindeutig Kennung des Objekts, das im übergeordneten Objekt enthalten ist.<br>Wenn zum Beispiel das RELATIONSHIP-Objekt eine Rollenmitgliedschaft beschreibt, wären die Elemente die Rollenmitglieder.<br>■ %ITEM_NAME% - Für den Benutzer sichtbarer Name der verschachtelten Gruppe. |
| USER | Ein gültiges Attribut, das für das USER-Objekt in der Verzeichniskonfigurationsdatei (directory.xml) definiert wird. |
| NONE | Keine Attribute. |

**Hinweis:** Folgende Punkte beziehen sich auf die vorangehende Tabelle:

- Für "enabled", "assignable", "auditable", "workflow", "hidden", "webservice" und "public" wird entweder "true" oder "false" protokolliert.
- Beim Überprüfen von Aufgaben für Rollen wird der für Benutzer sichtbare Name protokolliert.
- In der Datenbank sind Mitglieds-, Administrator- und Besitzerrichtlinien im kompilierten XML-Format gespeichert. Dieses Format unterscheidet sich von dem der Benutzeroberfläche, an der jede Richtlinie als ein Ausdruck angezeigt wird.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei der Management-Konsole an, wählen Sie die Umgebung und anschließend "Erweiterte Einstellungen" aus, und klicken Sie auf "Überprüfung".
2. Klicken Sie auf "Exportieren".

   Das System exportiert die aktuellen Auditeinstellungen in eine Auditeinstellungsdatei im XML-Format.

3. Ändern Sie die Auditeinstellungen in der XML-Datei, die Sie im vorherigen Schritt exportiert haben. Führen Sie folgende Aufgaben aus:

   a. Legen Sie den Wert für "Audit enabled" auf ="true" fest, und geben Sie den JNDI-Namenswert "iam_im_<auditdb>.xml" für die Element-Datenquelle an.

   b. Geben Sie den folgenden JNDI-Namen an:
   `java:/auditDbDataSource`

      **Hinweis**: Die Datenquelle befindet sich im folgenden Speicherort:
      `iam/im/jdbc/auditDbDataSource`

   c. Sie können Elemente in der Datei hinzufügen, ändern oder löschen.

   d. Ändern Sie die Ebene der für jedes Ereignis aufgezeichneten Informationen.

4. Wiederholen Sie Schritte 1 und 2. Klicken Sie auf "Importieren", und laden Sie die geänderte XML-Datei für Auditeinstellungen hoch.

5. Starten Sie die Umgebung neu.

Die Auditeinstellungsdatei ist jetzt aktualisiert.

## Aktivieren der Überwachung für eine Aufgabe

Aktivieren Sie die Überwachung für die Aufgaben, für die Sie die Überwachung in der Auditeinstellungsdatei konfiguriert haben.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei der Benutzerkonsole mit Systemadministratorrechten an.
2. Erstellen oder ändern Sie die Aufgabe, für die Sie Überwachung aktivieren möchten.
3. Stellen Sie auf der Registerkarte "Profil" sicher, dass das Kontrollkästchen "Überprüfung aktivieren" aktiviert ist.
4. Klicken Sie auf "Senden".

Die Überwachung ist jetzt zur Aufgabe aktiviert.

## Bericht anfordern

Um den Bericht anzuzeigen, fordern Sie einen Bericht bei einem Benutzer mit Berechtigungen zur Berichtsverwaltung an. Wählen Sie den entsprechenden Bericht aus, der die Audit-Daten verfolgt. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnmeldung.

Bevor Sie einen Bericht planen, führen Sie folgende Schritte aus:

1. Melden Sie sich bei der Benutzerkonsole mit Administratorrechten an.
2. Gehen Sie zu "Rollen und Aufgaben", "Admin-Aufgabe ändern", und wählen Sie eine Audit-Bericht aus, der geändert werden soll.
3. Wählen Sie die Registerkarte "Registerkarte" aus, und klicken Sie zur Bearbeitung auf "IAM ReportServerScheduler".
4. Aktivieren Sie das Kontrollkästchen "Option 'Wiederholungen' aktivieren".
5. Klicken Sie auf "OK" und auf "Senden".

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei der Benutzerkonsole mit Benutzerberechtigungen für Berichtsaufgaben an.
2. Wählen Sie "Berichte", "Berichtsaufgaben", "Bericht anfordern".

   Eine Liste der Berichte wird angezeigt.
3. Wählen Sie einen Audit-basierten Bericht aus.

   Ein Parameterfenster wird angezeigt.
4. Klicken Sie auf "Bericht planen", und wählen Sie einen Ablaufplan für Ihren Bericht aus.

   **Jetzt**

   Gibt an, dass der Bericht sofort ausgeführt wird.

   **Einmal**

   Gibt an, dass der Bericht einmal während eines bestimmten Zeitraums ausgeführt wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

   **(Nur Audit-Bericht) Stündlich**

   Gibt an, dass der Bericht zur Startzeit und dann alle "x" Stunden generiert wird; "x" gibt das Intervall zwischen den aufeinanderfolgenden Berichten an. Wählen Sie die Start- und Endzeit, das Start- und Enddatum und das Intervall zwischen aufeinanderfolgenden Berichten aus.

**(Nur Audit-Bericht) Täglich**

Gibt an, dass der Bericht zur Startzeit und dann alle "x" Tage generiert wird; "x" gibt das Intervall zwischen den aufeinanderfolgenden Berichten an. Wählen Sie die Start- und Endzeit, das Start- und Enddatum und das Intervall zwischen aufeinanderfolgenden Berichten aus.

**(Nur Audit-Bericht) Wöchentlich**

Gibt an, dass der Bericht ab dem ausgewählten Startdatum jede Woche zur Startzeit generiert wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

**(Nur Audit-Bericht) Monatlich**

Gibt an, dass der Bericht ab dem ausgewählten Startdatum jeden Monat und dann alle "x" Monate generiert wird. "x" bezeichnet das Intervall zwischen aufeinanderfolgenden Berichten. Wählen Sie die Start- und Endzeit, das Start- und Enddatum und das Intervall zwischen aufeinanderfolgenden Berichten aus.

**(Nur Audit-Bericht) Bericht an einem bestimmten Tag im Monat ausführen**

Gibt an, dass der Bericht am angegebenen Tag des angegebenen Monats generiert wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

**(Nur Audit-Bericht) Erster Montag**

Gibt an, dass der Bericht an jedem ersten Montag im Monat erstellt wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

**(Nur Audit-Bericht) Letzter Tag des Monats**

Gibt an, dass der Bericht am letzten Tag des Monats generiert wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus.

**(Nur Audit-Bericht) Tag X der Woche Y jeden Monats**

Gibt an, dass der Bericht an einem bestimmten Tag und in einer bestimmten Woche eines jeden Monats generiert wird. Wählen Sie zum Generieren des Berichts die Start- und Endzeit sowie das Start- und Enddatum aus. Sie können beispielsweise einen Bericht am Freitag in der dritten Woche eines jeden Monats generieren.

5. Klicken Sie auf "Senden".

   Die Berichtsanfrage wird gesendet. Je nach Umgebungskonfiguration wird die Anfrage sofort oder nach Genehmigung von einem Administrator ausgeführt.

   Normalerweise müssen ein Systemadministrator oder ein anderer Benutzer mit Berichtsverwaltungsberechtigungen eine Berichtsanfrage genehmigen, bevor das System sie fertig stellt. Eine Genehmigung ist erforderlich, weil einige Berichte eine lange Zeit oder bedeutende Systemressourcen benötigen können. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung.

   **Hinweis**: Aktivieren Sie WorkFlow für die Umgebung, wenn eine Genehmigung erforderlich ist.

## Anzeigen des Berichts

Je nach Umgebungskonfiguration wird ein Bericht zur Anzeige verfügbar, wenn ein Administrator die Anfrage für diesen Bericht genehmigt hat. Wenn Ihre Berichtsanfrage eine Genehmigung benötigt, sendet Ihnen das System eine E-Mail-Warnung. Der Bericht, den Sie anzeigen möchten, wird in der Suchliste nicht angezeigt, bis er genehmigt wird.

**Hinweis:** Damit Sie unter Verwendung der Aufgabe "Meine Berichte anzeigen" in CA IdentityMinder Berichte anzeigen können, müssen Sie in Ihrem Browser Sitzungscookies von Drittanbietern zulassen.

**Gehen Sie wie folgt vor:**

1. Wechseln Sie in der Benutzerkonsole zu "Berichte", "Berichtsaufgaben", und klicken Sie auf "Meine Berichte anzeigen".
2. Suchen Sie den generierten Bericht, den Sie anzeigen möchten.

   Es werden sowohl Wiederholungsberichte als auch Instanzen von Berichten bei Bedarf angezeigt.

   Hinweis: Wenn der Status des Berichts "Ausstehend/Wiederholend" lautet, wird der Bericht nicht generiert und es kann länger dauern, den Bericht abzuschließen.
3. Wählen Sie den Bericht aus, der angezeigt werden soll.
4. (Optional) Klicken Sie oben links auf "Diesen Bericht exportieren", um den Bericht in den folgenden Formaten zu exportieren:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) - nur Daten
   - Microsoft Excel (97-2003) - Bearbeitbar
   - Rich Text Format (RTF)
   - Getrennte Werte (CSV)
   - XML

# Bereinigen der Audit-Datenbank

In der Überprüfungsdatenbank können sich Datensätze ansammeln, die nicht mehr benötigt werden. Um diese Datensätze zu entfernen, führen Sie die folgende Datenbankprozedur im Verzeichnis "db\auditing" aus:

```
garbageCollectAuditing12 environment-ID MM/DD/YYYY
```

*Umgebungs-ID*

Gibt die ID der CA IdentityMinder-Umgebung an

*TT/MM/JJJJ*

Gibt das Datum an, vor dem Überprüfungsdatensätze gelöscht werden sollen.

# Kapitel 9: Produktionsumgebungen

Dieser Abschnitt enthält ausführliche Funktionsbeschreibungen für die Migration bestimmter Funktionskomponenten. Stellen Sie sicher, dass diese Möglichkeit nur genutzt wird, wenn in der Entwicklungsumgebung lediglich geringfügige Änderungen vorgenommen wurden und diese Änderungen bekannt sind.

Dieses Kapitel enthält folgende Themen:

So migrieren Sie Admin-Rollen und Aufgabendefinitionen (siehe Seite 265)
So migrieren Sie CA IdentityMinder-Designs (siehe Seite 267)
Aktualisieren von CA IdentityMinder in einer Produktionsumgebung (siehe Seite 268)
Migrieren der Datei "iam_im.ear" für JBoss (siehe Seite 270)
Migrieren der Datei "iam_im.ear" für WebLogic (siehe Seite 271)
Migrieren der Datei "iam_im.ear" für WebSphere (siehe Seite 272)
Migrieren von Workflow-Prozessdefinitionen (siehe Seite 274)

## So migrieren Sie Admin-Rollen und Aufgabendefinitionen

Sie können CA IdentityMinder-Rollen und -Aufgaben an die spezifischen Anforderungen Ihres Unternehmens anpassen. Diese Anpassungen beinhalten das Erstellen oder Ändern von Admin-Rollen und Aufgaben oder die Nutzung einer Erstellungs- bzw. Änderungsaufgabe für eine Admin-Rolle oder Aufgabe.

Eine andere Methode besteht darin, die Rollen und Aufgaben in der Datei "roledefinition.xml" zu ändern, allerdings wird diese *nicht empfohlen*. Aufgrund der Gefahr von Bearbeitungsfehlern sollten Sie diese Methode nur für sehr beschränkte Änderungen nutzen.

Bei diesem Prozess werden nur administrative Rollen- und Aufgabendefinitionen migriert. Wenn die Rollen an Organisationen gebunden wurden, sollten Sie eine Migration der gesamten CA IdentityMinder-Umgebung in Betracht ziehen.

**Wichtig!** Wenn Sie Rollen- oder Aufgabendefinitionen in der Produktionsumgebung geändert haben, gehen diese Änderungen beim Importieren der Rollen- oder Aufgabendefinitionen aus einer Entwicklungsumgebung verloren. Beim Importieren von Rollen- und Aufgabendefinitionen werden vorhandene Rollen- und Aufgabendefinitionen mit den selben Namen überschrieben.

## So exportieren Sie Admin-Rollen und Aufgabendefinitionen

Wenn Änderungen direkt in der Datei "roledefinition.xml" vorgenommen wurden, kann diese Datei unmittelbar in die Produktionsumgebung importiert werden. Gehen Sie andernfalls zum Exportieren der Rollen- und Aufgabendefinitionen wie folgt vor:

1. Wenn Sie ein Richtlinienserver-Cluster verwenden, müssen Sie überprüfen, dass nur ein Richtlinienserver ausgeführt wird.
2. Halten Sie bis auf einen alle CA IdentityMinder-Knoten an.
3. Melden Sie sich bei der Management-Konsole an.
4. Klicken Sie auf CA IdentityMinder-Umgebungen.
5. Wählen Sie die CA IdentityMinder-Umgebung aus, aus der die Rollen- und Aufgabendefinitionen exportiert werden sollen.
6. Klicken Sie auf "Rollen" und anschließend auf "Exportieren", und geben Sie einen Namen für die Datei ein.
7. Führen Sie die Anweisungen im nächsten Verfahren aus, um die so exportierte Datei zu importieren.

## So importieren Sie Admin-Rollen und Aufgabendefinitionen

**Gehen Sie wie folgt vor:**

1. Kopieren Sie die im vorangehenden Verfahren erstellte Datei in die Produktionsumgebung.
2. Melden Sie sich in der Produktionsumgebung an der Management-Konsole an.
3. Klicken Sie auf CA IdentityMinder-Umgebungen.
4. Wählen Sie die entsprechende CA IdentityMinder-Umgebung aus.
5. Klicken Sie auf "Rollen".
6. Klicken Sie auf "Importieren", und geben Sie den Namen der XML-Datei ein, die beim Export generiert wurde.
7. Wenn diese Schritte erfolgreich waren, starten Sie alle zusätzlichen Richtlinienserver und CA IdentityMinder-Knoten, die Sie angehalten hatten.

   **Hinweis:** Wenn weitere Änderungen in der CA IdentityMinder-Umgebung erforderlich sind, wiederholen Sie Schritt 6.

## So prüfen Sie den Rollen- und Aufgabenimport

Um zu prüfen, ob die Rollen und Aufgaben erfolgreich importiert wurden, melden Sie sich mit einem Administratorkonto bei CA IdentityMinder an, das die folgenden Aufgaben ausführen kann:

- Admin-Rolle ändern
- Admin-Aufgabe ändern

Führen Sie diese Aufgaben aus, und prüfen Sie, ob die Rollen und Aufgaben die neu importierten Rollendefinitionen widerspiegeln.

# So migrieren Sie CA IdentityMinder-Designs

Sie können die CA IdentityMinder-Designs anpassen, um der Anwendung ein bestimmtes Erscheinungsbild zu geben. Wenn Sie für eine Benutzergruppe Designs geändert oder neue Designs erstellt haben, führen Sie die folgenden Schritte aus, um die Designs von der Entwicklungs- auf die Produktionsumgebung zu migrieren.

Wenn Sie ein Design geändert haben, kopieren Sie die geänderten Dateien.

**Gehen Sie wie folgt vor:**

1. Kopieren Sie neue und geänderte Dateien vom Entwicklungs- auf den Produktionsserver, z. B. Bilddateien, Stylesheets, Eigenschaftsdateien und die Konsolenseite (index.jsp).
2. Wenn mehrere Designs verwendet werden, konfigurieren Sie eine SiteMinder-Antwort.

   **Hinweis**: Weitere Informationen über die Verwendung mehrerer Designs finden Sie im *Konfigurationshandbuch*.

Um die Migration der Designs zu prüfen, melden Sie sich an der Benutzerkonsole an, und prüfen Sie, ob das Design korrekt angezeigt wird.

# Aktualisieren von CA IdentityMinder in einer Produktionsumgebung

Nachdem Sie CA IdentityMinder von der Entwicklungs- auf die Produktionsumgebung migriert haben, müssen Sie ggf. inkrementelle Aktualisierungen durchführen. Führen Sie die folgenden Schritte aus, um neue CA IdentityMinder-Funktionen von Ihrer Entwicklungsumgebung auf Ihre Produktionsumgebung zu migrieren:

1. Migrieren Sie CA IdentityMinder-Umgebungen.
2. Kopieren Sie die Datei "iam_im.ear".
3. Migrieren Sie Workflow-Prozessdefinitionen.

## So migrieren Sie eine CA IdentityMinder-Umgebung

Eine CA IdentityMinder-Umgebung wird in der Management-Konsole erstellt. Eine CA IdentityMinder-Umgebung beinhaltet eine Reihe von Rollen- und Aufgabendefinitionen, Workflow-Definitionen, mit den CA IdentityMinder-APIs erstellte benutzerdefinierte Funktionen und ein CA IdentityMinder-Verzeichnis.

**Gehen Sie wie folgt vor:**

1. Wenn CA IdentityMinder mit SiteMinder integriert ist und Sie ein Richtlinienserver-Cluster verwenden, müssen Sie sicherstellen, dass nur ein Richtlinienserver ausgeführt wird.
2. Halten Sie bis auf einen alle CA IdentityMinder-Knoten an.
3. Exportieren Sie CA IdentityMinder-Umgebungen über die Management-Konsole aus der Entwicklungsumgebung.
4. Importieren Sie die exportierten Umgebungen über die Management-Konsole in die Produktionsumgebung.
5. Wenn CA IdentityMinder mit SiteMinder integriert ist, müssen Sie die CA IdentityMinder-Bereiche in der Benutzeroberfläche des Richtlinienservers erneut schützen.

   Die Richtliniendomäne wird beim Exportieren einer CA IdentityMinder-Umgebung nicht aus dem Richtlinienspeicher exportiert.
6. Starten Sie den Richtlinienserver und die CA IdentityMinder-Knoten neu, die Sie angehalten hatten.

Bei der Migration einer CA IdentityMinder-Umgebung werden die folgenden Aktivitäten ausgeführt:

- Wenn das gleiche Objekt an beiden Positionen vorhanden ist, überschreiben die Änderungen am Entwicklungsserver die Änderungen am Produktionsserver.
- Werden in der Entwicklungsumgebung neue Objekte erstellt, werden sie dem Produktionsserver hinzugefügt.
- Werden am Produktionsserver neue Objekte erstellt, werden sie beibehalten.

## So exportieren Sie eine CA IdentityMinder-Umgebung

Um eine CA IdentityMinder-Umgebung auf einem Produktionssystem bereitzustellen, exportieren Sie die Umgebung aus einem Entwicklungs- oder Staging-System, und importieren Sie sie in das Produktionssystem.

**Hinweis:** Wenn Sie eine zuvor exportierte Umgebung importieren, zeigt CA IdentityMinder ein Protokoll in einem Statusfenster in der Management-Konsole an. Um Validierungs- und Bereitstellungsinformationen für jedes verwaltete Objekt und seine Attribute in diesem Protokoll anzuzeigen, wählen Sie das Feld "Enable Verbose Log Output" (Ausführliche Protokollierungsausgabe aktivieren) auf der Seite "Environment Properties" (Umgebungseigenschaften) aus, *bevor* Sie die Umgebung exportieren. Die Auswahl des Felds "Enable Verbose Log Output" kann beträchtliche Leistungsprobleme beim Importieren verursachen.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Environments" (Umgebungen).

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

2. Wählen Sie die Umgebung aus, die Sie exportieren möchten.
3. Klicken Sie auf die Schaltfläche "Exportieren".

   Ein Dateidownload-Fenster wird angezeigt.

4. Speichern Sie die ZIP-Datei an einem Speicherort, auf den das Produktionssystem zugreifen kann.
5. Klicken Sie auf "Fertig stellen".

   Die Umgebungsinformationen werden in eine ZIP-Datei exportiert, die Sie in eine andere Umgebung importieren können.

## So importieren Sie eine CA IdentityMinder-Umgebung

Nachdem Sie eine CA IdentityMinder-Umgebung von einem Entwicklungssystem exportiert haben, können Sie sie in ein Produktionssystem importieren.

**Gehen Sie wie folgt vor:**

1. Klicken Sie in der Management-Konsole auf "Environments" (Umgebungen).

   Das CA IdentityMinder-Umgebungsfenster wird mit einer Liste von CA IdentityMinder-Umgebungen angezeigt.

2. Klicken Sie auf die Schaltfläche "Importieren".

   Das Fenster "Umgebung importieren" wird angezeigt.

3. Suchen Sie nach der entsprechenden ZIP-Datei, um eine Umgebung zu importieren.
4. Klicken Sie auf "Fertig stellen".

Die Umgebung wird in CA IdentityMinder importiert.

## So prüfen Sie die Migration einer CA IdentityMinder-Umgebung

Um zu prüfen, ob die CA IdentityMinder-Umgebung korrekt migriert wurde, stellen Sie sicher, dass die CA IdentityMinder-Umgebung in der Benutzeroberfläche des Richtlinienservers in der Produktionsumgebung angezeigt wird.

Prüfen Sie in der Benutzeroberfläche des Richtlinienservers die folgenden Punkte:

- Die Einstellungen des CA IdentityMinder-Benutzerverzeichnisses stimmen.
- Die neue CA IdentityMinder-Domäne ist vorhanden.
- Die richtigen Authentifizierungsschemen schützen die CA IdentityMinder-Bereiche.

Prüfen Sie nach der Anmeldung an der Management-Konsole außerdem, dass die CA IdentityMinder-Umgebung angezeigt wird, wenn Sie die Umgebungen auswählen.

# Migrieren der Datei "iam_im.ear" für JBoss

Sie müssen die Datei "iam_im.ear" jedes Mal erneut bereitstellen, wenn Funktionen von der Entwicklungsumgebung auf die Produktionsumgebung migriert werden. Durch die Migration der gesamten EAR-Datei stellen Sie sicher, dass die Entwicklungsumgebung mit der Produktionsumgebung identisch ist.

**Gehen Sie wie folgt vor:**

1. Kopieren Sie die Datei "iam_im.ear" von Ihrer Entwicklungsumgebung in ein Verzeichnis, auf das Ihre Produktionsumgebung Zugriff hat.
2. Bearbeiten Sie in der Kopie der Datei "iam_im.ear" die Verbindungsinformationen für den Richtlinienserver, sodass diese die Produktionsumgebung widerspiegeln.

   Um diese Änderung durchzuführen, kopieren Sie die Datei "*jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml" aus der Produktionsumgebung in die Datei "iam_im.ear".

3. Ersetzen Sie wie folgt die installierte Datei "iam_im.ear" durch die Kopie der Datei "iam_im.ear" aus der Entwicklungsumgebung:
   a. Löschen Sie auf dem Produktionsserver die Datei "iam_im.ear":

      *cluster_node_jboss_home*\server\default\deploy\iam_im.ear

   b. Ersetzen Sie die gelöschte Datei durch die bearbeitete Kopie der Datei "iam_im.ear" aus der Entwicklungsumgebung.
4. Wiederholen Sie diese Schritte für jeden Knoten im Cluster.

# Migrieren der Datei "iam_im.ear" für WebLogic

Sie müssen die Datei "iam_im.ear" jedes Mal erneut bereitstellen, wenn Funktionen von der Entwicklungsumgebung auf die Produktionsumgebung migriert werden. Durch die Migration der gesamten EAR-Datei stellen Sie sicher, dass die Entwicklungsumgebung mit der Produktionsumgebung identisch ist.

**Gehen Sie wie folgt vor:**

1. Behalten Sie die Verbindungsinformationen für den Richtlinienserver bei.

   Die Verbindungsinformationen für den Richtlinienserver werden in der Datei "ra.xml" im Verzeichnis "policyserver_rar/WEB-INF" gespeichert. Kopieren Sie diese Datei in ein anderes Verzeichnis, sodass diese in der Datei "iam_im.ear" vor der erneuten Bereitstellung ersetzt werden kann.

2. Kopieren Sie die Datei "iam_im.ear" in ein Verzeichnis, auf das der WebLogic-Admin-Server zugreifen kann.

3. Ersetzen Sie die Verbindungsinformationen für den Richtlinienserver.

   Ersetzen Sie in der Datei "iam_im.ear" die Datei "policyserver_rar/WEB-INF/ra.xml" durch die im Schritt 1 gespeicherte Datei.

4. Stellen Sie die Datei "iam_im.ear" erneut bereit.

   a. Melden Sie sich an der WebLogic-Konsole an.

   b. Wechseln Sie zu "Deployments" (Bereitsellungen), "Application" (Anwendung), "IdentityMinder".

Wählen Sie auf der Registerkarte "Deploy" (Bereitstellen) die Option "Deploy (Re-Deploy) Application" (Anwendung (erneut) bereitstellen) aus.

# Migrieren der Datei "iam_im.ear" für WebSphere

**Gehen Sie wie folgt vor:**

1. Kopieren Sie das Skript *imsInstall.jacl* aus dem Verzeichnis *was_im_tools_dir\WebSphere-tools* in das Verzeichnis *deployment_manager_dir \bin*. Dabei gilt:

   - *was_im_tools_dir* ist das Verzeichnis auf dem Entwicklungssystem, in dem die CA IdentityMinder-Tools für WebSphere installiert sind.

   - *deployment_manager_dir* ist das Verzeichnis, in dem der Bereitstellungsmanager installiert ist.

2. Kopieren Sie auf dem Entwicklungssystem, auf dem Sie die CA IdentityMinder-Anwendung konfiguriert haben, die Datei *was_im_tools_dir \WebSphere-tools\imsExport.bat* oder *imsExport.sh* in das Verzeichnis *was_home\bin.*

3. Navigieren Sie in der Befehlszeile zu *was_home\bin.*

4. Stellen Sie sicher, dass der WebSphere-Anwendungsserver ausgeführt wird.

5. Exportieren Sie die bereitgestellte CA IdentityMinder-Anwendung wie folgt:

   Geben Sie unter Windows den folgenden Befehl ein:

   ```
   imsExport.bat "path-to-exported-ear"
   ```

   Dabei steht *path-to-exported-ear* für den vollständigen Pfad und Dateinamen, die vom imsExport-Dienstprogramm erstellt wurden.

   Verwenden Sie für Windows-Systeme Schrägstriche (/) anstelle von umgekehrten Schrägstrichen (\), wenn Sie den Pfad zur Datei "was_im.ear" angeben. Beispiel:

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   Geben Sie unter UNIX den folgenden Befehl ein:

   ```
   ./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear
   ```

   Dabei steht *path-to-exported-ear* für den vollständigen Pfad, einschließlich Dateinamen, der exportierten EAR-Datei.

6. Kopieren Sie die exportierte EAR-Datei von dem Verzeichnis auf dem Entwicklungssystem, in das Sie diese exportiert haben, in ein Verzeichnis auf dem System, auf dem der Bereitstellungsmanager installiert ist.

7. Ersetzen Sie die Datei "*was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml" durch die aus der Produktionsumgebung.

   Die Datei "ra.xml" enthält die Verbindungsinformationen für den Richtlinienserver.

8. Stellen Sie auf dem System, auf dem der Bereitstellungsmanager installiert ist, die EAR-Datei von IdentityMinder bereit:

   a. Navigieren Sie in der Befehlszeile zu:

      *deployment_manager_dir* \bin.

   b. Stellen Sie sicher, dass der WebSphere-Anwendungsserver ausgeführt wird.

   c. Führen Sie das Skript "imsInstall.jacl" wie folgt aus:

   **Hinweis:** Die Ausführung des Skripts "imsInstall.jacl" kann mehrere Minuten in Anspruch nehmen.

   **Windows:**

   wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

   Dabei steht *path-to-copied-ear* für den vollständigen Pfad, einschließlich Dateinamen, der EAR-Datei von IdentityMinder, die Sie auf das Bereitstellungsmanagersystem kopiert haben.

   Beispiel:

   wsadmin -f imsInstall.jacl "c:\Programme\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

**UNIX:**

./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

Dabei steht *path-to-copied-ear* für den vollständigen Pfad, einschließlich Dateinamen, der EAR-Datei von IdentityMinder, die Sie auf das Bereitstellungsmanagersystem kopiert haben.

Beispiel:

./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. Wenn CA IdentityMinder mit SiteMinder integriert ist, prüfen Sie die folgenden Punkte:
   - Die SiteMinder-Agenten können eine Verbindung mit Ihrem Richtlinienspeicher herstellen.
   - Der Richtlinienserver kann eine Verbindung mit dem Benutzerspeicher herstellen.
   - Die CA IdentityMinder-Domänen wurden erstellt.

# Migrieren von Workflow-Prozessdefinitionen

Wenn Sie in der Entwicklungsumgebung einen Workflow verwendet haben, exportieren Sie die Workflow-Definitionen, und importieren Sie sie in die Produktionsumgebung. Konfigurieren Sie anschließend den Workflow in jedem Serverknoten.

## Exportieren von Prozessdefinitionen

Exportieren Sie die Workflow-Prozessdefinitionen auf dem Entwicklungsumgebungssystem.

**Gehen Sie wie folgt vor:**

1. Stellen Sie sicher, dass der Anwendungsserver ausgeführt wird.
2. Wechseln Sie in das Verzeichnis " *admin_tools*\Workpoint\bin\", und führen Sie die Datei "Archive.bat" (für Windows) oder "Archive.sh" (für UNIX) wie folgt aus:
   a. Wählen Sie im Dialogfeld "Importieren" das Stammobjekt aus.
   b. Klicken Sie auf "Hinzufügen".
   c. Geben Sie den Namen der zu generierenden Datei an.

d. Klicken Sie auf "Exportieren".

e. Klicken Sie auf "Los".

*admin_tools* bezieht sich auf die Verwaltungstools, die standardmäßig in einem der folgenden Verzeichnisse installiert werden:

- **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

3. Führen Sie die Anweisungen im nächsten Abschnitt Importieren von Prozessdefinitionen (siehe Seite 275) aus.

## Importieren von Prozessdefinitionen

Importieren Sie auf dem Produktionsumgebungssystem die Workflow-Prozessdefinitionen.

**Gehen Sie wie folgt vor:**

1. Starten Sie den Anwendungsserver neu.
2. Erstellen Sie optional eine Sicherungskopie der aktuellen Definitionen, indem Sie die Definitionen mithilfe des vorangehenden Verfahrens exportieren.
3. Wechseln Sie in das Verzeichnis "*admin_tools*\Workpoint\bin\", und führen Sie das Archive-Skript wie folgt aus:

   a. Wählen Sie im Dialogfeld "Importieren" alle zu importierenden Elemente aus.

   b. Wenn Sie gefragt werden, ob das neue oder das alte Format verwendet werden soll, behalten Sie das alte Format bei.

   CA IdentityMinder wird von dem neuen Format nicht unterstützt.

   c. Geben Sie den Namen der durch den Export generierten Datei an.

   d. Klicken Sie auf "Los".

   *admin_tools* bezieht sich auf die Verwaltungstools, die standardmäßig in einem der folgenden Verzeichnisse installiert werden:

   - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

# Kapitel 10: CA IdentityMinder-Protokolle

Dieses Kapitel enthält folgende Themen:

So verfolgen Sie Probleme in CA IdentityMinder (siehe Seite 277)
So verfolgen Sie Komponenten und Datenfelder (siehe Seite 279)

## So verfolgen Sie Probleme in CA IdentityMinder

CA IdentityMinder beinhaltet die folgenden Methoden zum Aufzeichnen des Status und Nachverfolgen von Problemen:

**Die Aufgabe "Gesendete Aufgaben anzeigen"**

Zeigt den Status aller Ereignisse und Aufgaben in einer CA IdentityMinder-Umgebung an. Administratoren verwenden diese Aufgabe in der Benutzerkonsole.

Durch "Gesendete Aufgaben anzeigen" werden die folgenden Arten von Informationen bereitgestellt:

- Die Liste der Ereignisse und Aufgabe in der Umgebung
- Die Liste der Attribute, die einem Ereignis zugeordnet sind
- Erfolgreiche und fehlgeschlagene Ereignisse
- Ausstehende oder blockierte Ereignisse
- Abgelehnte Ereignisse, einschließlich des Grundes für die Ablehnung
- Status der Kontosynchronisierung
- Status der Identitätsrichtliniensynchronisierung
- Bereitstellungsinformationen (wenn die Bereitstellung aktiviert ist)

**Anwendungsserverprotokolle**

Diese Protokolle zeigen Informationen zu allen Komponenten in einer CA IdentityMinder-Installation an und enthalten Details zu allen Vorgängen in CA IdentityMinder.

Der Speicherort und Typ der Protokolldatei hängt davon ab, welchen der folgenden Anwendungsservertypen Sie verwenden:

- WebLogic - CA IdentityMinder-Informationen werden in die Standardausgabe geschrieben. Die Standardausgabe ist normalerweise das Konsolenfenster, in dem die Serverinstanz ausgeführt wird.
- JBoss - CA IdentityMinder-Informationen werden in das Konsolenfenster, in dem die Serverinstanz ausgeführt wird, und in die Datei "*jboss_home*\server\log\server.log" geschrieben.
- WebSphere - CA IdentityMinder-Informationen werden in das Konsolenfenster, in dem die Serverinstanz ausgeführt wird, und in die Datei "*was_home*\AppServer\logs*server_name*\SystemOut" geschrieben.

Weitere Informationen finden Sie in der Dokumentation zu Ihrem Anwendungsserver.

**Verzeichnisserver-Protokolldatei**

Enthält Informationen zu Aktivitäten im Benutzerverzeichnis.

Die Art der aufgezeichneten Informationen und der Speicherort der Protokolldatei hängen vom Typ des verwendeten Verzeichnisservers ab. Weitere Informationen finden Sie in der Dokumentation zum Verzeichnisserver.

**Richtlinienserver-Protokolldatei**

Zeigt die folgenden Informationen an, wenn CA IdentityMinder mit SiteMinder integriert ist:

- SiteMinder-Verbindungsprobleme
- SiteMinder-Authentifizierungsprobleme
- Information zu verwalteten Objekte von CA IdentityMinder im SiteMinder-Richtlinienspeicher
- Kennwortrichtlinienauswertung

Weitere Informationen zum Konfigurieren von SiteMinder-Protokollen finden Sie im *CA SiteMinder Web Access Manager Policy Server-Administrationshandbuch*.

**Richtlinienserver-Profiler**

Ermöglicht Ihnen bei einer Integration von CA IdentityMinder mit SiteMinder die Nachverfolgung von Diagnose- und Verarbeitungsfunktionen des internen Richtlinienservers, einschließlich auf CA IdentityMinder bezogener Funktionen.

Weitere Informationen finden Sie unter So verfolgen Sie Komponenten und Datenfelder (siehe Seite 279).

**Web-Agent-Protokolldateien**

Wenn CA IdentityMinder mit SiteMinder integriert ist, schreiben die Web-Agenten Informationen in die beiden folgenden Protokolle:

- Fehlerprotokolldatei - Diese enthält Fehler auf Programm- und Betriebsebene, zum Beispiel wenn der Web-Agent keine Verbindung mit dem Richtlinienserver herstellen kann.
- Verfolgungsprotokolldatei - Diese enthält Warnungen und Informationsmeldungen, wie Ablaufverfolgungsmeldungen und Ablaufstatusmeldungen. Darüber hinaus sind Daten wie Headerdetails und Cookievariablen hierin eingeschlossen.

**Hinweis:** Weitere Informationen zu Web-Agent-Protokolldateien finden Sie im *CA SiteMinder Web Access Manager Web Agent-Konfigurationshandbuch*.

# So verfolgen Sie Komponenten und Datenfelder

Wenn CA IdentityMinder mit SiteMinder integriert ist, können Sie den Richtlinienserver-Profiler von SiteMinder verwenden, um Komponenten und Datenfelder in den CA IdentityMinder-Erweiterungen für den Richtlinienserver zu verfolgen. Mithilfe des Profilers können Sie Filter für die Ablaufverfolgungsausgabe konfigurieren, sodass nur bestimmte Werte für eine Komponente oder ein Datenfeld erfasst werden.

**Hinweis:** Anweisungen zur Verwendung des Richtlinienserver-Profilers finden Sie im *CA SiteMinder Web Access Manager Policy Server-Administrationshandbuch*.

Sie können die Ablaufverfolgung für die folgenden Komponenten aktivieren:

**Function_Begin_End**

Stellt untergeordnete Ablaufverfolgungsanweisungen bereit, wenn gewisse Methoden in den CA IdentityMinder-Erweiterungen für den Richtlinienserver ausgeführt werden.

**IM_Error**

Verfolgt Laufzeitfehler in den CA IdentityMinder-Erweiterungen für den SiteMinder-Richtlinienserver.

**IM_Info**

Stellt allgemeine Ablaufverfolgungsinformationen für die CA IdentityMinder-Erweiterungen bereit.

**IM_Internal**

Verfolgt allgemeine Informationen über interne CA IdentityMinder-Vorgänge.

**IM_MetaData**

Stellt Ablaufverfolgungsinformationen bereit, wenn CA IdentityMinder die Verzeichnismetadaten verarbeitet.

**IM_RDB_Sql**

Stellt Ablaufverfolgungsinformationen für relationale Datenbanken bereit.

**IM_LDAP_Provider**

Stellt Ablaufverfolgungsinformationen für LDAP-Verzeichnisse bereit.

**IM_RuleParser**

Verfolgt die Analyse und Auswertung von in einer XML-Datei definierten Mitglieder-, Besitzer- und Admin-Richtlinien, die zur Laufzeit interpretiert werden.

**IM_RuleEvaluation**

Verfolgt die Auswertung von Mitglieder-, Admin-, Besitzer- und Bereichsregeln.

**IM_MemberPolicy**

Verfolgt die Auswertung von Mitgliederrichtlinien, einschließlich Mitgliedschaft und Bereich.

**IM_AdminPolicy**

Verfolgt die Auswertung von Admin-Richtlinien.

**IM_OwnerPolicy**

Verfolgt die Auswertung von Besitzerrichtlinien.

**IM_RoleMembership**

Verfolgt Informationen bezüglich der Rollenmitgliedschaft, wie die Liste der Rollen eines Benutzer und die Liste der Mitglieder in einer bestimmten Rolle.

**IM_RoleAdmins**

Verfolgt Informationen bezüglich der Rollenverwaltung, wie die Liste der Rollen, die ein Benutzer verwalten kann, und die Liste der Administratoren für eine bestimmte Rolle.

**IM_RoleOwners**

Verfolgt Informationen bezüglich des Rollenbesitzes, wie die Liste der Rollen, die ein Benutzer besitzt, und die Liste der Besitzer für eine bestimmte Rolle.

**IM_PolicyServerRules**

Verfolgt die Auswertung von Mitgliederregeln, wie RoleMember, RoleAdmin und RoleOwner, die der Richtlinienserver aufgelöst hat, und von Bereichsregeln, wie All und AccessTaskFilter, für Zugriffsaufgaben.

**IM_LLSDK_Command**

Verfolgt die Kommunikation zwischen dem internen CA IdentityMinder-SDK und dem Richtlinienserver. Der technische Support verwendet diese Verfolgungskomponente.

**IM_LLSDK_Message**

Verfolgt, ob Meldungen mittels Java-Code explizit vom internen CA IdentityMinder-SDK an den Richtlinienserver gesendet werden. Der technische Support verwendet diese Verfolgungskomponente.

**IM_IdentityPolicy**

Verfolgt die Auswertung und Anwendung von Identitätsrichtlinien.

**IM_PasswordPolicy**

Verfolgt die Auswertung von Kennwortrichtlinien.

**IM_Version**

Stellt Informationen zur CA IdentityMinder-Version bereit.

**IM_CertificationPolicy**

Verfolgt die Auswertung von Zertifizierungsrichtlinien.

**IM_InMemoryEval**

Verfolgt die Verarbeitung von CA IdentityMinder-Richtlinien, einschließlich Mitglieder-, Admin-, Besitzer- und Identitätsrichtlinien. Der technische Support verwendet diese Verfolgungskomponente.

**IM_InMemoryEvalDetail**

Stellt zusätzliche Informationen zur Verarbeitung von CA IdentityMinder-Richtlinien bereit, einschließlich Mitglieder-, Admin-, Besitzer- und Identitätsrichtlinien. Der technische Support verwendet diese Verfolgungskomponente.

Die Datenfelder, für die Sie die Ablaufverfolgung konfigurieren können, werden im *CA SiteMinder Web Access Manager Policy Server-Administrationshandbuch* aufgeführt.

# Kapitel 11: CA IdentityMinder-Schutz

Dieses Kapitel enthält folgende Themen:

Sicherheit an der Benutzerkonsole (siehe Seite 283)
Sicherheit an der Management-Konsole (siehe Seite 284)
Schutz vor CSRF-Angriffen (siehe Seite 289)

## Sicherheit an der Benutzerkonsole

Die Benutzerkonsole ist die Benutzeroberfläche, an der Administratoren Objekte wie Benutzer, Gruppen und Organisationen in einer CA IdentityMinder-Umgebung verwalten können. Diesen Objekten wird ein Satz zugehöriger Rollen und Aufgaben zugeordnet. Wenn sich ein Administrator an der Benutzerkonsole anmeldet, werden die mit dem Administrator verknüpften Aufgaben in dieser Umgebung angezeigt.

Standardmäßig schränkt CA IdentityMinder den Zugriff auf die Benutzerkonsole mittels einer systemeigenen Authentifizierung ein. CA IdentityMinder-Administratoren müssen einen gültigen Benutzernamen und ein Kennwort eingeben, um sich an einer CA IdentityMinder-Umgebung anzumelden. CA IdentityMinder authentifiziert den Namen und das Kennwort mithilfe des Benutzerspeichers, den CA IdentityMinder verwaltet.

Wenn allerdings CA IdentityMinder mit SiteMinder integriert ist, verwendet CA IdentityMinder *automatisch* die grundlegende SiteMinder-Authentifizierung, um die Umgebung zu schützen. Es ist keine zusätzliche Konfiguration erforderlich, um die grundlegende Authentifizierung zu verwenden. Sie können jedoch erweiterte Authentifizierungsmethoden mithilfe der administrativen SiteMinder-Benutzeroberfläche konfigurieren.

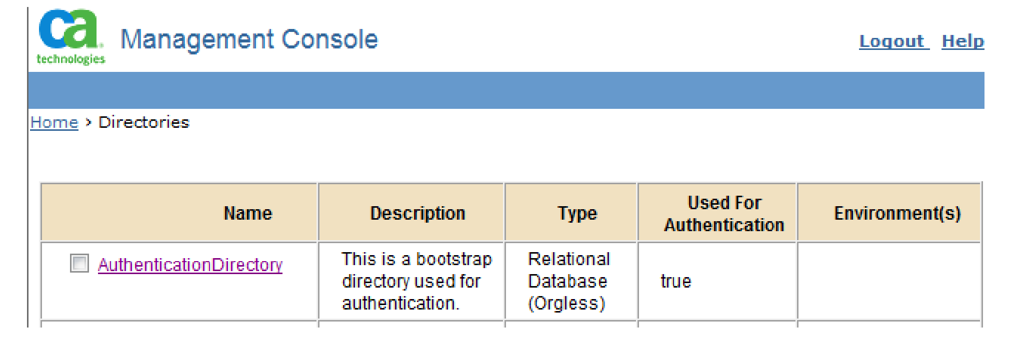
**Hinweis:** Weitere Informationen finden Sie im *CA SiteMinder Web Access Manager Policy Server-Konfigurationshandbuch*.

# Sicherheit an der Management-Konsole

Die Management-Konsole ermöglicht Administratoren, CA IdentityMinder-Verzeichnisse und -Umgebungen zu erstellen und zu verwalten. Darüber hinaus können Administratoren die Management-Konsole verwenden, um benutzerdefinierte Funktionen für eine Umgebung zu konfigurieren.

Die CA IdentityMinder-Installation beinhaltet eine Option zum Schutz der Management-Konsole. Diese Option ist standardmäßig aktiviert. Während der Installation geben Sie Anmeldeinformationen an, die CA IdentityMinder zum Authentifizieren eines Administrators verwendet, der auf die Management-Konsole zugreifen kann. CA IdentityMinder erstellt einen Benutzer mit den Anmeldeinformationen, die Sie in einem Bootstrap-Verzeichnis namens "AuthenticationDirectory" angeben. Sie können dieses Verzeichnis in der Management-Konsole anzeigen.

**Hinweis:** Sie können die systemeigene Sicherheit nicht verwenden, um die Management-Konsole zu schützen, wenn CA IdentityMinder mit CA SiteMinder integriert ist.



## Hinzufügen zusätzlicher Administratoren zur Management-Konsole

Standardmäßig hat eine Management-Konsole, die durch die systemeigene CA IdentityMinder-Sicherheit geschützt wird, ein Administratorkonto, das während der Installation in einem neuen CA IdentityMinder-Verzeichnis erstellt wird.

Um zusätzliche Administratoren hinzuzufügen, geben Sie ein CA IdentityMinder-Verzeichnis an, das die Benutzer enthält, die Zugriff auf die Management-Konsole haben sollen. Durch die Verwendung eines vorhandenen Verzeichnisses können Sie Benutzern in Ihrer Organisation Zugriff auf die Management-Konsole erteilen, ohne dass Sie neue Konten erstellen müssen.

Sie können nur ein Verzeichnis für die Authentifizierung angeben. Ein Verzeichnis, das für die Authentifizierung konfiguriert ist, kann nicht gelöscht werden.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich mit den während der Installation angegebenen Benutzeranmeldeinformationen an der Management-Konsole an.
2. Öffnen Sie "Directories", und klicken Sie auf das Verzeichnis mit den Benutzern, die Zugriff auf die Management-Konsole benötigen.
3. Klicken Sie auf "Update Authentication".
4. Wählen Sie die Option "Used for Authentication" aus.
5. Geben Sie den Benutzernamen des ersten Benutzers ein, und klicken Sie auf "Add".
6. Fügen Sie weitere Benutzer hinzu, die Zugriff auf die Management-Konsole benötigen, bis alle Benutzer hinzugefügt wurden. Klicken Sie dann auf "Speichern".

   Die angegebenen Benutzer können nun mit ihrem Benutzernamen und Kennwort auf die Management-Konsole zugreifen.

## Deaktivieren der systemeigenen Sicherheit für die Management-Konsole

Wenn Sie die systemeigene Sicherheit für die Management-Konsole aktiviert haben und jetzt eine andere Anwendung zum Schutz der Management-Konsole verwenden möchten, müssen Sie die systemeigene Sicherheit deaktivieren, bevor Sie eine andere Sicherheitsmethode implementieren.

**Gehen Sie wie folgt vor:**

1. Deaktivieren Sie die systemeigene Sicherheit für die Management-Konsole in der Datei "web.xml" wie folgt:
   a. Öffnen Sie die Datei "*CA IdentityMinder_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml" in einem Texteditor.
   b. Legen Sie den Wert des Parameters "Enable" für "ManagementConsoleAuthFilter" wie folgt auf "false" fest:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-class>com.netegrity.ims.manage.filter.ManagementCon
   soleAuthFilter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>false</param-value>
   </init-param>
   </filter>
   ```
   c. Speichern Sie die Datei "web.xml".
2. Starten Sie den CA IdentityMinder-Server neu.

   Die Management-Konsole ist nicht mehr durch die systemeigene Sicherheit geschützt.

## Schützen der Management-Konsole mit SiteMinder

Um die Management-Konsole von Anfang an zu schützen, können Sie eine SiteMinder-Richtlinie erstellen.

Eine SiteMinder-Richtlinie kennzeichnet eine Ressource, die Sie schützen möchten, z. B. die Management-Konsole, und erteilt einer Gruppe von Benutzern Zugriff auf diese Ressource.

**Gehen Sie wie folgt vor:**

1. Deaktivieren Sie die systemeigene Sicherheit (siehe Seite 286) für die Management-Konsole.
2. Melden Sie sich bei einer der folgenden Schnittstellen als Administrator mit Domänenberechtigungen an:
   - Für CA SiteMinder r12 oder höher melden Sie sich bei der Verwaltungsoberfläche an.
   - Melden Sie sich bei CA SiteMinder 6.0 SP*x* an der Benutzeroberfläche des Richtlinienservers an.

   **Hinweis:** Weitere Informationen zur Verwendung dieser Schnittstellen finden Sie in der Dokumentation der SiteMinder-Version, die Sie verwenden.
3. Suchen Sie die Richtliniendomäne für die jeweilige CA IdentityMinder-Umgebung.

   Diese Domäne wird automatisch erstellt, wenn CA IdentityMinder mit SiteMinder integriert ist. Der Domänenname hat das folgende Format:

   *Identity Manager-Umgebung*Domain

   Dabei steht *Identity Manager-environment* für den Namen der Umgebung, die Sie ändern. Wenn zum Beispiel der Name *employees* ist, lautet der Domänenname "*employees*Domain".
4. Erstellen Sie einen Bereich mit dem folgenden Ressourcenfilter:

   /iam/immanage/
5. Erstellen Sie eine Regel für den Bereich. Geben Sie ein Sternchen (*) als Filter an, um alle Seiten in der Management-Konsole zu schützen.
6. Erstellen Sie eine neue Richtlinie, und ordnen Sie sie der Regel zu, die Sie im vorherigen Schritt erstellt haben.

   Stellen Sie sicher, dass Sie Benutzer zuordnen, die mithilfe der Richtlinie auf die Management-Konsole zugreifen können.
7. Starten Sie den Anwendungsserver neu.

## Schützen einer vorhandenen Umgebung nach einem Upgrade

Nach einem Upgrade auf CA IdentityMinder 12.6 oder höher können Sie die Management-Konsole mithilfe der systemeigenen Sicherheit schützen.

**Hinweis:** Sie können die systemeigene CA IdentityMinder-Sicherheit nicht verwenden, um die Management-Konsole zu schützen, wenn CA IdentityMinder mit CA SiteMinder integriert ist.

**Gehen Sie wie folgt vor:**

1. Aktivieren Sie die systemeigene Sicherheit für die Management-Konsole in der Datei "web.xml" wie folgt:
   a. Öffnen Sie die Datei "*CA IdentityMinder_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml" in einem Texteditor.
   b. Legen Sie den Wert des Parameters "Enable" für "ManagementConsoleAuthFilter" wie folgt auf "true" fest:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-class>com.netegrity.ims.manage.filter.ManagementConsoleAuthFilter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>true</param-value>
   </init-param>
   </filter>
   ```
   c. Speichern Sie die Datei "web.xml".
2. Erstellen Sie die Tabelle IM_AUTH_USER im CA IdentityMinder-Objektspeicher.

   In der Tabelle IM_AUTH_USER werden Informationen zu den Administratoren in der Management-Konsole gespeichert.
   a. Wechseln Sie in das Verzeichnis "CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore".
   b. Führen Sie eines der folgenden Skripte für den Objektspeicher aus:
      - sql_objectstore.sql
      - oracle_objectstore.sql

   **Hinweis:** Weitere Informationen zum Ausführen eines Skripts für eine vorhandene Datenbank finden Sie in der Herstellerdokumentation zur jeweiligen Datenbank.

3. Verwenden Sie das Kennwort-Tool, um das Kennwort zu verschlüsseln.

   Das Kennwort-Tool ist mit den CA IdentityMinder-Tools im folgenden Speicherort installiert:

Windows - C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   Führen Sie das Kennwort-Tool mithilfe des folgenden Befehls aus:
   `pwdtools -JSAFE -p` *`anypassword`*

   Die JSAFE-Option verschlüsselt einen einfachen Textwert unter Verwendung des PBE-Algorithmus.

1. Fügen Sie die Bootstrap-Benutzerinformationen in die Tabelle IM_AUTH_USER ein. Geben Sie Werte für alle Spalten in der Tabelle IM_AUTH_USER an.

   Beispiel:

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. Starten Sie den CA IdentityMinder-Server neu.

   Die Management-Konsole ist durch die systemeigene Sicherheit geschützt.

# Schutz vor CSRF-Angriffen

CA IdentityMinder wurde erweitert, um den Schutz vor CSRF-Angriffen (Cross-Site Request Forgery, websiteübergreifende Anforderungsfälschung) zu verbessern. Standardmäßig ist diese Erweiterung in CA IdentityMinder deaktiviert.

So aktivieren Sie die Erweiterung:

1. Öffnen Sie die Datei "web.xml" in folgendem Verzeichnis:

   *`application-server`*`/iam_im.ear/user_console.war/WEB-INF`

2. Suchen Sie das <context-param>-Element mit der Angabe "<param-name> csrf-prevention-on".
3. Legen Sie für "<param-value>" den Wert "true" fest.
4. Starten Sie den Anwendungsserver neu.

# Kapitel 12: Integration von CA SiteMinder

Dieses Kapitel enthält folgende Themen:


SiteMinder und CA IdentityMinder (siehe Seite 292)
So schützen Sie Ressourcen (siehe Seite 293)
Übersicht über die Integration von SiteMinder und CA IdentityMinder (siehe Seite 294)
Konfigurieren des SiteMinder-Richtlinienspeichers für CA IdentityMinder (siehe Seite 299)
Importieren des CA IdentityMinder-Schemas in den Richtlinienspeicher (siehe Seite 306)
Erstellen eines SiteMinder 4.X-Agentenobjekts (siehe Seite 306)
Exportieren der CA IdentityMinder-Verzeichnisse und Umgebungen (siehe Seite 308)
Löschen aller Verzeichnis- und Umgebungsdefinitionen (siehe Seite 309)
Aktivieren des SiteMinder-Richtlinienserver-Ressourcenadapters (siehe Seite 310)
Deaktivieren des systemeigenen CA IdentityMinder-Framework-Authentifizierungsfilter (siehe Seite 311)
Neustarten des Anwendungsservers (siehe Seite 312)
Konfigurieren einer Datenquelle für SiteMinder (siehe Seite 312)
Importieren der Verzeichnisdefinitionen (siehe Seite 313)
Aktualisieren und Importieren von Umgebungsdefinitionen (siehe Seite 314)
Installieren des Web-Proxyserver-Plug-ins (siehe Seite 314)
Ordnen Sie den SiteMinder-Agenten einer CA IdentityMinder-Domäne zu (siehe Seite 335)
Konfigurieren des SiteMinder-Parameters "LogOffUrl" (siehe Seite 336)
Fehlerbehebung (siehe Seite 336)
So konfigurieren Sie CA IdentityMinder-Agent-Einstellungen (siehe Seite 346)
Konfigurieren der SiteMinder-Hochverfügbarkeit (siehe Seite 347)
Entfernen von SiteMinder aus einer vorhandenen CA IdentityMinder-Bereitstellung (siehe Seite 350)
SiteMinder-Vorgänge (siehe Seite 350)

# SiteMinder und CA IdentityMinder

Bei Integration von CA IdentityMinder und CA SiteMinder kann CA SiteMinder die CA IdentityMinder-Umgebung um die folgenden Funktionen ergänzen:

**Erweiterte Authentifizierung**

CA IdentityMinder beinhaltet standardmäßig eine systemeigene Authentifizierung für CA IdentityMinder-Umgebungen. CA IdentityMinder-Administratoren müssen einen gültigen Benutzernamen und ein Kennwort eingeben, um sich an einer CA IdentityMinder-Umgebung anzumelden. CA IdentityMinder authentifiziert den Namen und das Kennwort mithilfe des Benutzerspeichers, den CA IdentityMinder verwaltet.

Wenn CA IdentityMinder mit CA SiteMinder integriert ist, verwendet CA IdentityMinder die grundlegende CA SiteMinder-Authentifizierung, um die Umgebung zu schützen. Beim Erstellen einer CA IdentityMinder-Umgebung werden in CA SiteMinder eine Richtliniendomäne und ein Authentifizierungsschema erstellt, um diese Umgebung zu schützen.

Ist CA IdentityMinder mit CA SiteMinder integriert, können Sie auch die SiteMinder-Authentifizierung verwenden, um die Management-Konsole zu schützen.

**Zugriffsrollen und -aufgaben**

Zugriffsrollen ermöglichen CA IdentityMinder-Administratoren, Berechtigungen in Anwendungen zuzuweisen, die von CA SiteMinder geschützt werden. Diese Zugriffsrollen stellen eine einzelne Aktion dar, die ein Benutzer in einer Geschäftsanwendung ausführen kann, wie beispielsweise eine Bestellung in einer Finanzanwendung zu generieren.

**Verzeichniszuordnung**

Ein Administrator muss möglicherweise Benutzer verwalten, deren Profile in einem anderen als dem für die Authentifizierung des Administrators verwendeten Benutzerspeicher enthalten sind. Bei der Anmeldung an der CA IdentityMinder-Umgebung wird der Administrator mithilfe eines Verzeichnisses authentifiziert, und ein anderes Verzeichnis berechtigt den Administrator, Benutzer zu verwalten.

Bei Integration von CA IdentityMinder und CA SiteMinder können Sie eine CA IdentityMinder-Umgebung so konfigurieren, dass unterschiedliche Verzeichnisse für Authentifizierung und Autorisierung verwendet werden.

**Designs für unterschiedliche Benutzergruppen**

Ein Design ändert das Erscheinungsbild der Benutzerkonsole. Bei Integration von CA IdentityMinder und CA SiteMinder können Sie festlegen, dass unterschiedlichen Benutzergruppen unterschiedliche Designs angezeigt werden. Um diese Änderung durchzuführen, verwenden Sie zum Zuordnen eines Designs zu einer Benutzergruppe eine SiteMinder-Antwort. Die Antwort ist mit einer Regel in einer Richtlinie verknüpft, die einem Satz von Benutzern zugeordnet ist. Wenn die Regel ausgelöst wird, wird wiederum die Antwort ausgelöst, um an CA IdentityMinder Informationen zum Design weiterzugeben, mit dem die Benutzerkonsole erstellt werden soll.

**Hinweis:** Weitere Informationen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**Gebietsschemavoreinstellungen für eine lokalisierte Umgebung**

Bei Integration von CA IdentityMinder und CA SiteMinder können Sie mithilfe des HTTP-Headers "Imlanguage" Gebietsschemavoreinstellungen für einen Benutzer definieren. Sie legen diesen Header am SiteMinder-Richtlinienserver innerhalb einer SiteMinder-Antwort fest und geben ein Benutzerattribut als Wert des Headers an. Dieser Imlanguage-Header dient als Gebietsschemavoreinstellung höchster Priorität für einen Benutzer.

**Hinweis:** Weitere Informationen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

**Weitere Informationen:**

Erfassen von Benutzeranmeldeinformationen mithilfe eines benutzerdefinierten Authentifizierungsschemas (siehe Seite 351)

# So schützen Sie Ressourcen

Für die erweiterte Authentifizierung benötigen Sie einen SiteMinder-Richtlinienserver in Ihrer Implementierung. Der Anwendungsserver, der den CA IdentityMinder-Server hostet, befindet sich in einer anderen Betriebsumgebung als der Webserver. Um den Weiterleitungsdienst bereitzustellen, benötigt der Webserver Folgendes:

- Ein vom Hersteller des Anwendungsservers bereitgestelltes Plug-in.
- Einen SiteMinder-Agenten, um die CA IdentityMinder-Ressourcen zu schützen, z. B. eine Benutzerkonsole oder Funktionen für die Selbstregistrierung oder für vergessene Kennwörter.

Der Web-Agent steuert den Zugriff von Benutzern, die CA IdentityMinder-Ressourcen anfordern. Nachdem die Benutzer authentifiziert und autorisiert wurden, lässt der Web-Agent zu, dass der Webserver die Anforderungen verarbeitet.

Wenn der Webserver die Anforderung empfängt, leitet das Anwendungsserver-Plug-in diese an den Anwendungsserver weiter, der den CA IdentityMinder-Server hostet.

Der Web-Agent schützt die CA IdentityMinder-Ressourcen, die für Benutzer und Administratoren offengelegt werden.

# Übersicht über die Integration von SiteMinder und CA IdentityMinder

Wenn der Richtlinienadministrator und der Identitätsadministrator zusammenarbeiten, um SiteMinder in eine vorhandene CA IdentityMinder-Installation zu integrieren, wird die CA IdentityMinder-Architektur um die folgenden Komponenten erweitert:

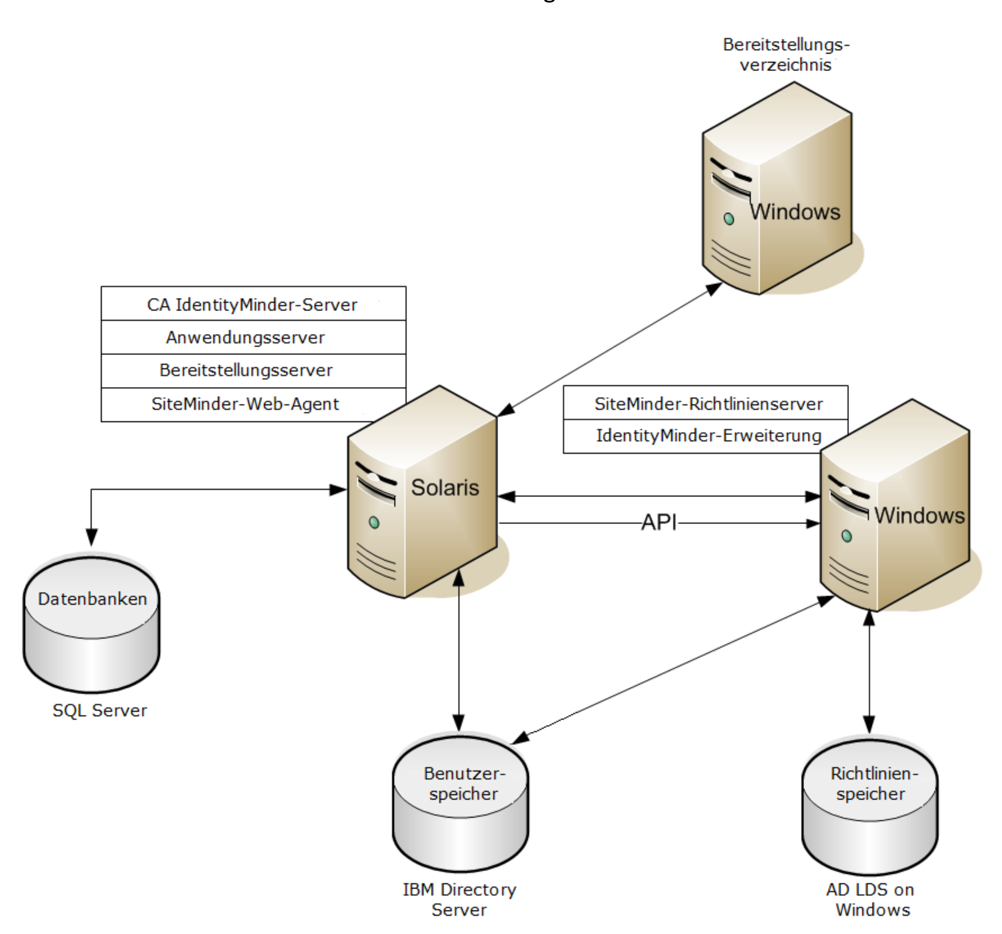
**SiteMinder-Web-Agent**

Schützt den CA IdentityMinder-Server. Der Web-Agent wird auf dem System mit dem CA IdentityMinder-Server installiert.

**SiteMinder-Richtlinienserver**

Stellt eine erweiterte Authentifizierung und Autorisierung für CA IdentityMinder bereit.

Die folgende Abbildung zeigt ein Beispiel für eine CA IdentityMinder-Installation mit einem SiteMinder-Richtlinienserver und -Web-Agenten:

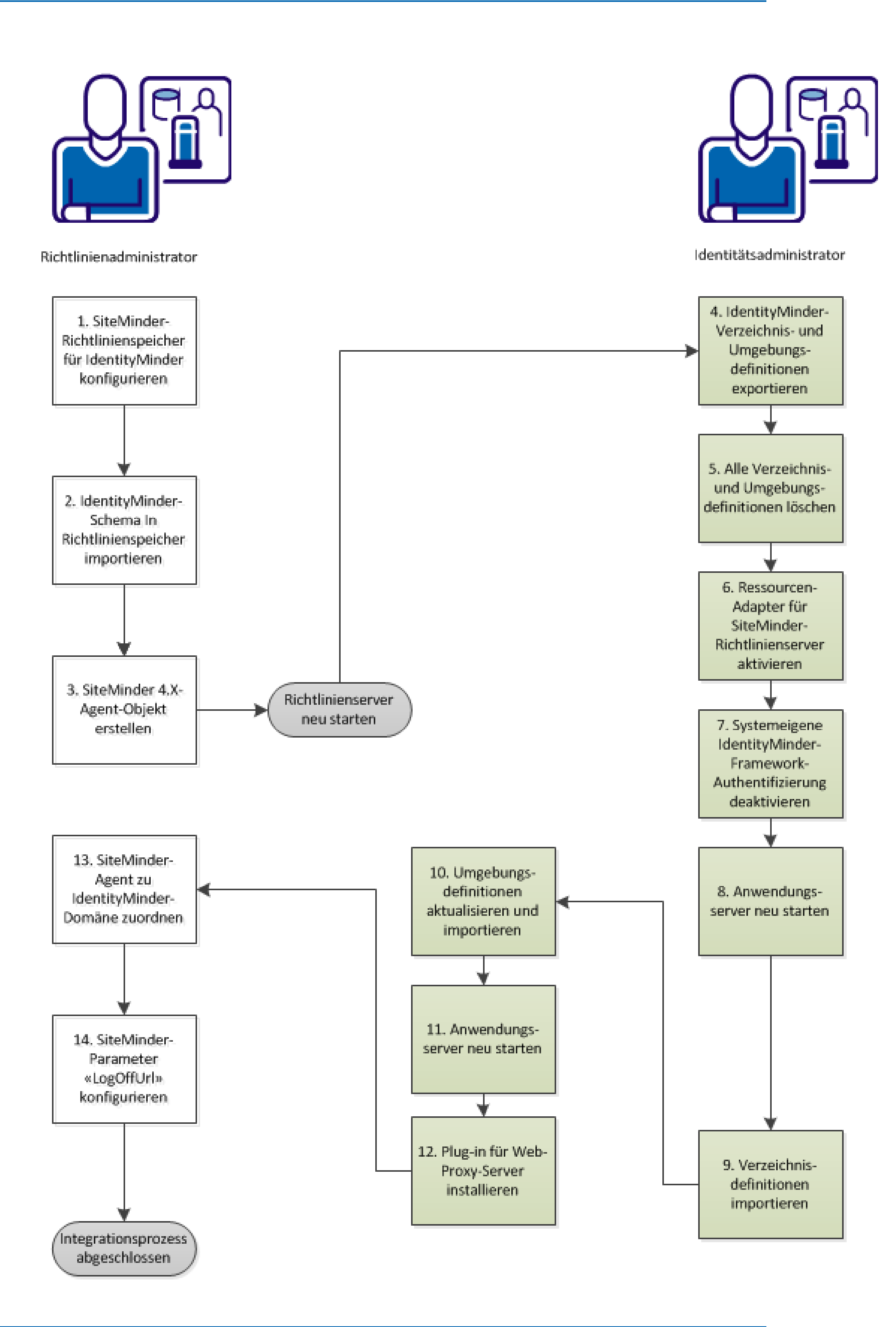



**Hinweis**: Die Komponenten werden als Beispiele auf unterschiedlichen Plattformen installiert. Allerdings können Sie andere Plattformen wählen. Die CA IdentityMinder-Datenbanken befinden sich auf Microsoft SQL Server und der Benutzerspeicher auf IBM Directory Server. Der SiteMinder-Richtlinienspeicher befindet sich auf AD LDS unter Windows.

Für diesen Prozess werden zwei Rollen benötigt: der CA IdentityMinder-Identitätsadministrator und der SiteMinder-Richtlinienadministrator. In manchen Organisationen hat eine Person beide Rollen inne. Wenn zwei Personen an dem Prozess beteiligt sind, ist für die Verfahren in diesem Szenario eine enge Zusammenarbeit erforderlich. Der Richtlinienadministrator beginnt und beendet diesen Prozess, während der Identitätsadministrator die Schritte dazwischen ausführt.

**Wichtig!** Für CA IdentityMinder-Installationen ab Release 12.5 SP7 werden Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files (JCE-Bibliotheken) benötigt. Laden Sie diese Bibliotheken von der Oracle-Website herunter. Laden Sie sie in den folgenden Ordner: <Java_path>\<jdk_version>\jre\lib\security\.

Das folgende Diagramm veranschaulicht den gesamten Prozess zur Integration von SiteMinder und CA IdentityMinder:



Richtlinienadministrator
Identitätsadministrator
1. SiteMinder-Richtlinienspeicher für IdentityMinder konfigurieren
2. IdentityMinder-Schema in Richtlinienspeicher importieren
3. SiteMinder 4.X-Agent-Objekt erstellen
Richtlinienserver neu starten
4. IdentityMinder-Verzeichnis- und Umgebungs-definitionen exportieren
5. Alle Verzeichnis- und Umgebungs-definitionen löschen
6. Ressourcen-Adapter für SiteMinder-Richtlinienserver aktivieren
7. Systemeigene IdentityMinder-Framework-Authentifizierung deaktivieren
8. Anwendungs-server neu starten
9. Verzeichnis-definitionen importieren
10. Umgebungs-definitionen aktualisieren und importieren
11. Anwendungs-server neu starten
12. Plug-in für Web-Proxy-Server installieren
13. SiteMinder-Agent zu IdentityMinder-Domäne zuordnen
14. SiteMinder-Parameter «LogOffUrl» konfigurieren
Integrationsprozess abgeschlossen

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie den SiteMinder-Richtlinienspeicher für CA IdentityMinder. (siehe Seite 299)
2. Importieren Sie das CA IdentityMinder-Schema in den Richtlinienspeicher. (siehe Seite 306)
3. Erstellen Sie ein SiteMinder 4.X-Agentenobjekt. (siehe Seite 306)
4. Exportieren Sie die CA IdentityMinder-Verzeichnisse und -Umgebungen. (siehe Seite 308)
5. Löschen Sie alle Verzeichnis- und Umgebungsdefinitionen. (siehe Seite 309)
6. Aktivieren Sie den Ressourcenadapter des SiteMinder-Richtlinienservers. (siehe Seite 310)
7. Deaktivieren Sie den systemeigenen CA IdentityMinder Framework Authentication Filter. (siehe Seite 311)
8. Starten Sie den Anwendungsserver neu. (siehe Seite 312)
9. Konfigurieren Sie eine Datenquelle für SiteMinder. (siehe Seite 312)
10. Importieren Sie die Verzeichnisdefinitionen. (siehe Seite 313)
11. Aktualisieren und importieren Sie die Umgebungsdefinitionen. (siehe Seite 314)
12. Starten Sie den Anwendungsserver neu. (siehe Seite 312)
13. Installieren Sie das Web-Proxy-Server-Plug-in. (siehe Seite 314)
14. Ordnen Sie den SiteMinder-Agenten einer CA IdentityMinder-Domäne zu. (siehe Seite 335)
15. Konfigurieren Sie den Parameter "LogOffUrl" in SiteMinder. (siehe Seite 336)

# Konfigurieren des SiteMinder-Richtlinienspeichers für CA IdentityMinder

Als Richtlinienadministrator verwenden Sie die CA IdentityMinder-Verwaltungstools, um auf SQL-Skripte oder LDAP-Schematext zuzugreifen und das IMS-Schema dem Richtlinienspeicher hinzuzufügen. Der Identitätsadministrator hat diese Tools im Ordner "Admin Tools" installiert. Führen Sie *eines* der folgenden Verfahren durch, um den Richtlinienspeicher zu konfigurieren:

Konfigurieren einer relationalen Datenbank (siehe Seite 300)

Konfigurieren von Sun Java Systems Directory Server oder IBM Directory Server (siehe Seite 300)

Konfigurieren von Microsoft Active Directory (siehe Seite 301)

Konfigurieren von Microsoft ADAM (siehe Seite 302)

Konfigurieren von CA Directory Server (siehe Seite 302)

Konfigurieren von Novell eDirectory Server (siehe Seite 304)

Konfigurieren von Oracle Internet Directory (OID) (siehe Seite 305)

## Konfigurieren einer relationalen Datenbank

Nach der Konfiguration können Sie die relationale Datenbank als SiteMinder-Richtlinienspeicher verwenden.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie die Datenbank als einen unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Anweisungen zur Konfiguration finden Sie im *Installationshandbuch zum SiteMinder-Richtlinienserver.*

2. Führen Sie das entsprechende Skript für Ihre Datenbank aus:

   - **SQL:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   Die vorangehenden Pfade sind die Standardinstallationsverzeichnisse. Der Speicherort für Ihre Installation kann hiervon abweichen.

## Konfigurieren von Sun Java Systems Directory Server oder IBM Directory Server

Zum Konfigurieren eines Java oder IBM Verzeichnisservers wenden Sie die entsprechende Schemadatei an.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

2. Fügen Sie dem Verzeichnis die entsprechende LDIF-Schemadatei hinzu. Der Standardspeicherort für die LDIF-Dateien unter Windows ist "C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas".

   Fügen Sie die folgenden Schemadateien für Ihr Verzeichnis hinzu:

   - **IBM Directory Server:**

     IBMDirectoryServer\V3.identityminder8

   - **Sun Java Systems Directory Server (iPlanet):**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

## Konfigurieren von Microsoft Active Directory

Um einen Microsoft Active Directory-Richtlinienspeicher zu konfigurieren, wenden Sie das Skript "activedirectory_ims8.ldif" an.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

2. Ändern Sie die Schemadatei "activedirectory_ims8.ldif" wie folgt:

   a. Öffnen Sie die Datei "activedirectory_ims8.ldif" in einem Texteditor. Der Standardspeicherort unter Windows ist:

      C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Ersetzen Sie alle Instanzen von "{root}" durch die Stammorganisation für das Verzeichnis.

      Die Stammorganisation muss mit der Stammorganisation übereinstimmen, die Sie beim Konfigurieren des Richtlinienspeichers in der Richtlinienserver-Management-Konsole angegeben haben.

      Wenn zum Beispiel die Stammorganisation "dc=myorg,dc=com" ist, ersetzen Sie "
      dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root}" durch "dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com".

   c. Speichern Sie die Datei.

3. Fügen Sie die Schemadatei entsprechend der Beschreibung in der Dokumentation zu Ihrem Verzeichnis hinzu.

## Konfigurieren von Microsoft ADAM

Um einen Microsoft ADAM-Richtlinienspeicher zu konfigurieren, wenden Sie das Skript "adam_ims8.ldif" an.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

   Notieren Sie den CN-Wert (die GUID).

2. Ändern Sie die Schemadatei "adam_ims8.ldif" wie folgt:

   a. Öffnen Sie die Datei "adam_ims8.ldif" in einem Texteditor. Der Standardspeicherort unter Windows ist:

      C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Ersetzen Sie jeden Verweis auf "cn={guid}" durch die Zeichenfolge, die Sie beim Konfigurieren des SiteMinder-Richtlinienspeichers in Schritt 1 dieses Verfahrens notiert haben.

      Wenn zum Beispiel die GUID-Zeichenfolge "CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}" ist, dann ersetzen Sie jeden Verweis auf "cn={guid}" durch "CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}".

   c. Speichern Sie die Datei.

3. Fügen Sie die Schemadatei entsprechend der Beschreibung in der Dokumentation zu Ihrem Verzeichnis hinzu.

## Konfigurieren von CA Directory Server

Um CA Directory Server zu konfigurieren, erstellen Sie eine benutzerdefinierte Schemadatei. In den nachfolgenden Schritten ist *dxserver_home* das Verzeichnis, in dem CA Directory installiert ist. Das Standardinstallationsverzeichnis für diese Datei unter Windows ist "C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory".

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

2. Kopieren Sie die Datei "etrust_ims8.dxc" in das Verzeichnis "*dxserver_home*\config\schema".

3. Erstellen Sie wie folgt eine benutzerdefinierte Schemakonfigurationsdatei:

   a. Kopieren Sie die Datei "*dxserver_home*\config\schema\default.dxg" nach "*dxserver_home*\config\schema*company_name*-schema.dxg*".*

   b. Bearbeiten Sie die Datei "*dxserver_home*\config\schema*company_name*-schema.dxg", indem Sie am Ende der Datei die folgenden Zeilen einfügen:

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Bearbeiten Sie die Datei "*dxserver_home*\bin\schema.txt", indem Sie den Inhalt der Datei *"*etrust_ims_schema.txt" am Ende der Datei einfügen. Das Standardinstallationsverzeichnis für diese Datei unter Windows ist "C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory".

5. Erstellen Sie wie folgt eine benutzerdefinierte Beschränkungskonfigurationsdatei:

   a. Kopieren Sie die Datei "*dxserver_home*\config\limits\default.dxc" nach "*dxserver_home*\config\limits*company_name*-limits.dxc".

   b. Erhöhen Sie die Standardgrößenbeschränkung in der Datei "*dxserver_home*\config\limits*company_name-limits*.dxc" wie folgt auf 5.000:

   ```
   set max-op-size=5000
   ```

   **Hinweis:** Beim Upgrade von CA Directory wird die Datei "limits.dxc" überschrieben. Stellen Sie daher sicher, dass Sie nach Abschluss des Upgrades den Wert von "max-op-size" auf 5.000 zurücksetzen.

6. Bearbeiten Sie die Datei "*dxserver_home*\config\servers*dsa_name*.dxi" wie folgt:

   ```
   # schema
   source "company_name-schema.dxg";

   #service limits
   source "company_name-limits.dxc";
   ```

   Dabei steht *dsa_name* für den Namen des DSA bei Verwendung der angepassten Konfigurationsdateien.

7. Führen Sie das Dienstprogramm "dxsyntax" aus.

8. Halten Sie wie folgt den DSA an, und starten Sie ihn als DSA-Benutzer neu, damit die Schemaänderungen wirksam werden::

   ```
   dxserver stop dsa_name
   dxserver start dsa_name
   ```

## Konfigurieren von Novell eDirectory Server

Um einen Novell eDirectory Server-Richtlinienspeicher zu konfigurieren, wenden Sie das Skript "novell_ims8.ldif" an.

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

2. Suchen Sie den definierten Namen (DN) des NCPServer für Novell eDirectory Server, indem Sie die folgenden Informationen in ein Befehlsfenster auf dem System eingeben, auf dem der Richtlinienserver installiert ist:

   ```
   ldapsearch -h hostname -p port -b container -s sub
   -D admin_login -w password objectClass=ncpServer dn
   ```

   Beispiel:

   ```
   ldapsearch -h 192,168.1,47 -p 389 -b "o=nwqa47container" -s sub -D
   "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
   ```

3. Öffnen Sie die Datei "novell_ims8.ldif"..

4. Ersetzen Sie jede NCPServer-Variable durch den in Schritt 2 ermittelten Wert.

   Der Standardspeicherort der Datei "novell_ims8.ldif" unter Windows ist:

   C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory

   Wenn zum Beispiel der DN-Wert "cn=servername,o=servercontainer" ist, würden Sie jede Instanz von *NCPServer* durch "cn=servername,o=servercontainer" ersetzen.

5. Aktualisieren Sie eDirectory Server mit der Datei "novell_ims8.ldif".

   Anweisungen hierzu finden Sie in der Dokumentation zu Novell eDirectory.

## Konfigurieren von Oracle Internet Directory (OID)

Um Oracle Internet Directory zu konfigurieren, aktualisieren Sie die Datei "oracleoid.ldif".

**Gehen Sie wie folgt vor:**

1. Konfigurieren Sie das Verzeichnis als unterstützten SiteMinder-Richtlinienspeicher.

   **Hinweis:** Konfigurationsanweisungen finden Sie im *Installationshandbuch zum CA SiteMinder-Richtlinienserver*.

2. Aktualisieren Sie Oracle Internet Directory Server mit der Datei "oracleoid_ims8.ldif". Das Standardinstallationsverzeichnis für diese Datei unter Windows ist:

   *install_path*\policystore-schemas\OracleOID\

   Anweisungen hierzu finden Sie in der Dokumentation zu Oracle Internet Directory.

## Prüfen des Richtlinienspeichers

Um den Richtlinienspeicher zu prüfen, bestätigen Sie die folgenden Punkte:

- Das Richtlinienserverprotokoll enthält keinen Abschnitt mit Warnungen, der mit dem folgenden Code beginnt:

  ```
  *** IMS NO SCHEMA BEGIN
  ```

  Diese Warnung wird nur angezeigt, wenn Sie die Erweiterungen für den SiteMinder-Richtlinienserver installiert, aber das Richtlinienspeicherschema nicht erweitert haben.

- Die CA IdentityMinder-Objekte sind in der Datenbank oder dem Verzeichnis des Richtlinienspeichers vorhanden. Die CA IdentityMinder-Objekte fangen mit dem Präfix "ims" an.

# Importieren des CA IdentityMinder-Schemas in den Richtlinienspeicher

Der Richtlinienadministrator importiert das CA IdentityMinder-Schema in den Richtlinienspeicher. Durch diese Aufgabe kann CA IdentityMinder Richtlinienobjekte erstellen, aktualisieren und löschen. Beispiele hierfür sind Verzeichnisobjekte, Domänen, Bereiche, Regeln, Richtlinien und die Richtlinienobjekte, die Zugriffsrollen und -aufgaben aktivieren.

**Gehen Sie wie folgt vor:**

1. Beenden Sie auf dem SiteMinder-Richtlinienserver den Richtlinienserverdienst.
2. Führen Sie das CA IdentityMinder-Installationsprogramm für die Version aus, die Sie verwenden.
3. Wenn Sie gefragt werden, welche Komponenten Sie installieren möchten, wählen Sie die Erweiterungen für SiteMinder aus (wenn SiteMinder lokal installiert ist).
4. Stellen Sie sicher, dass der Richtlinienserverdienst neu gestartet wurde, bevor Sie fortfahren.

# Erstellen eines SiteMinder 4.X-Agentenobjekts

Der Richtlinienadministrator erstellt einen SiteMinder 4.x-Web-Agenten. Diese Aufgabe ermöglicht die Kommunikation zwischen SiteMinder und CA IdentityMinder. Der Identitätsadministrator bezieht sich während der CA IdentityMinder-Konfiguration auf diesen Agenten.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich auf der SiteMinder-Verwaltungsoberfläche an.

   Die entsprechenden Registerkarten für Ihre Administratorrechte werden angezeigt.
2. Klicken Sie auf "Infrastruktur", "Agenten", "Agent", "Agent erstellen".

   Das Dialogfeld "Agent erstellen" wird angezeigt.
3. Wählen Sie "Neues Objekt des Typs 'Agent' erstellen" aus, und klicken Sie dann auf "OK".

   Das Dialogfeld "Agent erstellen" wird angezeigt.
4. Geben Sie einen Namen und eine optionale Beschreibung ein.

   **Hinweis:** Verwenden Sie einen Namen, den Sie leicht zum entsprechenden SharePoint-Verbindungsassistenten zuordnen können.

5. Wählen Sie "SiteMinder".
6. Wählen Sie "Web-Agent" aus der Dropdown-Liste aus.
7. Aktivieren Sie die 4.x-Funktionalität mit den folgenden Schritten:
   a. Aktivieren Sie das Kontrollkästchen "Unterstützt 4.x-Agenten".

      Die Vertrauenseinstellungsfelder werden angezeigt.
   b. Fügen Sie die Vertrauenseinstellungen durch das Ausfüllen der folgenden Felder hinzu:

      IP-Adresse

      Enthält die IP-Adresse des Richtlinienservers.

      Gemeinsamer geheimer Schlüssel

      Gibt ein Kennwort an, das dem 4.x-Agent-Objekt zugeordnet wird. Der SharePoint-Verbindungsassistent benötigt dieses Kennwort ebenfalls.

      Geheimen Schlüssel bestätigen

      Bestätigt ein Kennwort, das dem 4.x-Agent-Objekt zugeordnet wird. Der SharePoint-Verbindungsassistent benötigt auch die Bestätigung von diesem Kennwort.
8. Klicken Sie auf "Senden".

   Die Aufgabe zum Erstellen des Agent-Objekts wird zur Verarbeitung übermittelt und die Bestätigungsmeldung erscheint.

# Exportieren der CA IdentityMinder-Verzeichnisse und Umgebungen

Der Integrationsprozess entfernt alle aktuellen Umgebungs- und Verzeichnisdefinitionen. Um sicherzustellen, dass diese Informationen beibehalten werden, exportiert der Identitätsadministrator die Umgebungen mithilfe der CA IdentityMinder-Management-Konsole. Nachdem Sie die Integration abgeschlossen haben, stellen diese Definitionen die Verzeichnisse und Umgebungen wieder her.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die CA IdentityMinder-Management-Konsole.
2. Klicken Sie auf "Directories" (Verzeichnisse).
3. Klicken Sie auf das erste Verzeichnis in der Liste und dann auf "Export".
4. Speichern und archivieren Sie die Verzeichnis-xml-Datei.
5. Wiederholen Sie diesen Vorgang für die verbleibenden Verzeichnisse.
6. Klicken Sie auf "Startseite" und dann auf "Umgebungen".
7. Wählen Sie die erste Umgebung aus.
8. Klicken Sie auf "Exportieren".
9. Wiederholen Sie diesen Vorgang für die verbleibenden Umgebungen.

   **Hinweis:** Dieser Prozess kann ein paar Minuten für jede Umgebung dauern.

# Löschen aller Verzeichnis- und Umgebungsdefinitionen

Um SiteMinder für den Schutz von CA IdentityMinder vorzubereiten, löscht der Identitätsadministrator die Verzeichnis- und Umgebungsdefinitionen mithilfe der CA IdentityMinder-Management-Konsole.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie die CA IdentityMinder-Management-Konsole.
2. Klicken Sie auf "Umgebungen".
3. Wählen Sie die erste Umgebung aus.
4. Klicken Sie auf "Löschen".
5. Wiederholen Sie diesen Prozess für jede Ihrer verbleibenden Umgebungen.

   **Hinweis:** Löschen Sie die Umgebungen, bevor Sie Ihre Verzeichnisse löschen, weil die Umgebungen sich auf die Verzeichnisse beziehen.
6. Navigieren Sie zurück zum Abschnitt der Verzeichnisse.
7. Wählen Sie alle aufgelisteten Verzeichnisse aus.
8. Klicken Sie auf "Löschen".

# Aktivieren des SiteMinder-Richtlinienserver-Ressourcenadapters

Der Identitätsadministrator aktiviert den SiteMinder-Richtlinienserver-Ressourcenadapter. Der Zweck des Adapters ist, den SMSESSION-Cookie zu validieren. Nach der Validierung erstellt SiteMinder den Benutzerkontext.

**Gehen Sie wie folgt vor:**

1. Navigieren Sie zum Ordner "\policysever.rar\META-INF" in "iam_im.ear" auf dem Anwendungsserver, der CA IdentityMinder ausführt.
2. Öffnen Sie die Datei "ra.xml" in einem Editor.
3. Suchen Sie nach "config-property" "Enabled", und ändern Sie dann den Wert von "config-property" zu "true", wie im folgenden Beispiel gezeigt:

```
        <config-property-name>ValidateSMHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. Suchen Sie die ConnectionURL-Eigenschaft, und geben Sie den Hostnamen des SiteMinder-Richtlinienservers an. Verwenden Sie einen vollqualifizierten Domänennamen (FQDN).
5. Suchen Sie die UserName-Eigenschaft, und geben Sie das für die Kommunikation mit SiteMinder zu verwendende Konto an. SiteMinder ist der Standardwert für dieses Konto.
6. Suchen Sie die AdminSecret-Eigenschaft. Geben Sie das verschlüsselte Kennwort an. Kopieren Sie das Kennwort aus der Datei "directory.xml", die Sie exportiert haben, und fügen Sie es in "ra.xml" ein. Wenn Sie nicht sicher sind, ob Sie ein gebräuchliches Kennwort haben, verschlüsseln Sie Ihr Kennwort mithilfe des CA IdentityMinder-Kennwort-Tools.
7. Fügen Sie das verschlüsselte Kennwort in die Datei "ra.xml" ein.
8. Geben Sie den 4.x-Agentennamen an, den der Richtlinienadministrator während der SiteMinder-Konfiguration erstellt hat.

9. Geben Sie das verschlüsselte Kennwort an. Verwenden Sie das Kennwort-Tool, um das Kennwort im Bedarfsfall zu verschlüsseln.
10. Speichern Sie die Änderungen an der ra.xml-Datei.

Der SiteMinder-Richtlinienserver-Ressourcenadapter wird aktiviert.

**Weitere Informationen:**

Ändern eines SiteMinder-Kennworts oder gemeinsamen geheimen Schlüssels (siehe Seite 371)

# Deaktivieren des systemeigenen CA IdentityMinder-Framework-Authentifizierungsfilter

Mit dem SiteMinder-Adapter an Ort und Stelle wird der Framework-Authentifizierungsfilter nicht mehr benötigt. Der Identitätsadministrator kann den Filter deaktivieren.

**Gehen Sie wie folgt vor:**

1. Suchen und bearbeiten Sie die Datei "web.xml" im Ordner "\user_console.war\WEB-INF" unter "iam_im.ear".
2. Suchen Sie "FrameworkAuthFilter" und ändern Sie den Wert von "Enable init-param" zu "false".

   Wenn Sie CA IdentityMinder r12.5 SP 7 oder höher verwenden, überprüfen Sie, dass die Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files (JCE) in das Verzeichnis "\<Java_path>\<jdk_version>\jre\lib\security" in der CA IdentityMinder-Umgebung heruntergeladen wurden. Diese Dateien ermöglichen CA IdentityMinder, mit SiteMinder Verbindung aufzunehmen.

   Wenn die JCE-Bibliotheken installiert werden, sehen Sie während des CA IdentityMinder-Anwendungsstarts die folgenden Meldungen:

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Startup Step 2 : Attempting to start PolicyServerService
   2012-07-06 11:23:56,081 WARN [ims.default] (main) Unlimited Strength Java Crypto Extensions enabled: TRUE
   ```

   Andernfalls ist der Wert für den Eintrag "Unlimited Strength Java Crypto Extensions enabled" "false". CA IdentityMinder kann dann keine Verbindung mit dem Richtlinienserver aufnehmen.

# Neustarten des Anwendungsservers

Der Neustart aktualisiert den Anwendungsserver mit den Änderungen. Der Identitätsadministrator validiert, dass der Wechsel erfolgreich war und dass eine ordnungsgemäße Verbindung zum SiteMinder-Richtlinienserver besteht.

**Gehen Sie wie folgt vor:**

1. Verwenden Sie den Services-Bereich, um CA IdentityMinder neu zu starten, wenn Ihr Anwendungsserver als Service ausgeführt wird.
2. Überprüfen Sie "server.log", um die Verbindung zu validieren

# Konfigurieren einer Datenquelle für SiteMinder

Wenn Ihre CA IdentityMinder-Umgebung eine relationale Datenbank für seinen Identitätsspeicher verwendet, ist der Identitätsadministrator erforderlich, um einen zusätzlichen Prozess auf dem SiteMinder-Richtlinienserver abzuschließen. SiteMinder erfordert, dass eine lokale Datenquelle mit der Datenbank kommuniziert.

**Gehen Sie wie folgt vor:**

1. Öffnen Sie für Windows-Server die ODBC-Datenquellen-Administratorkonsole, die sich unter den Verwaltungstools befindet.
2. Klicken Sie auf die Registerkarte "System-DSN".
3. Klicken Sie auf "Hinzufügen", und wählen Sie den entsprechenden SiteMinder-Treiber für Ihre Datenbank aus.
4. Geben Sie die benötigten Informationen an, um auf den Benutzerspeicher der relationalen Datenbank zu verweisen.
5. Testen Sie die Konnektivität, bevor Sie fortfahren.

# Importieren der Verzeichnisdefinitionen

Um das Importieren der Umgebungen vorzubereiten, importiert der Identitätsadministrator die Verzeichnisse, auf die die Umgebungen verweisen. Beim Importieren der Verzeichnisdefinition in CA IdentityMinder werden außerdem die Verzeichnisinformationen zum SiteMinder-Richtlinienspeicher hinzugefügt.

**Gehen Sie wie folgt vor:**

1. Stellen Sie sicher, dass CA IdentityMinder ausgeführt wird und mit SiteMinder verbunden ist.
2. Navigieren Sie zur CA IdentityMinder-Management-Konsole.
3. Klicken Sie auf "Directories" (Verzeichnisse) und dann auf "Create or Update from XML" (Aus XML erstellen oder aktualisieren).
4. Wählen Sie Ihre Verzeichniskonfigurationsdatei aus (directory.xml). Diese Datei ist diejenige, welche Sie in Exportieren der CA IdentityMinder-Verzeichnisse und Umgebungen (siehe Seite 308) exportiert haben.
5. Klicken Sie auf Weiter.
6. Klicken Sie auf "Fertig stellen", und überprüfen Sie die Lastausgabe. Vergewissern Sie sich, dass das Verzeichnis in CA IdentityMinder und SiteMinder vorhanden ist.
7. Wiederholen Sie diese Schritte für den Bereitstellungsspeicher und verbleibende Verzeichnisse.
8. Melden Sie sich bei der SiteMinder-Verwaltungsoberfläche an, um die Erstellung der Benutzerverzeichnisse zu validieren.

# Aktualisieren und Importieren von Umgebungsdefinitionen

Der Identitätsadministrator importiert die aktualisierten Umgebungen zurück in CA IdentityMinder.

**Gehen Sie wie folgt vor:**

1. Im Gegensatz zu den Verzeichnisexporten ist der Umgebungsexport in Form einer ZIP-Datei. Ziehen Sie eine Kopie der *name*.xml-Datei aus der ZIP-Datei.
2. Kopieren Sie die *name*.xml-Datei. Fügen Sie am Ende des Elements "ImsEnvironment" einen Verweis auf den Schutzagenten (nicht der SM-4.x-Agent) ein, vor der schließenden Klammer />: *agent="idmadmin"*
3. Speichern und fügen Sie die Datei zurück in die ZIP-Datei ein.
4. Öffnen Sie die CA IdentityMinder-Management-Konsole, klicken Sie auf "Umgebungen" und dann auf "Import".
5. Geben Sie den Namen der aktualisierten Umgebungs-ZIP-Datei ein.
6. Klicken Sie auf "Fertig stellen", und überprüfen Sie die Importausgabe.
7. Wiederholen Sie diesen Prozess für alle Ihre verbleibenden Umgebungen.
8. Starten Sie den Anwendungsserver neu.

# Installieren des Web-Proxyserver-Plug-ins

Basieren auf der installierten Anwendung installiert der Identitätsadministrator eines der folgenden Plug-ins, die der Webserver verwendet, um Anfragen an den Anwendungsserver weiterzuleiten:

- WebSphere (siehe Seite 315)
- JBoss (siehe Seite 323)
- WebLogic (siehe Seite 327)

## Installieren des Proxy-Plug-ins auf WebSphere

Der Webserver, auf dem Sie den Web-Agent installiert haben, leitet Anfragen an den Anwendungsserver weiter, der den CA IdentityMinder-Server hostet. Das vom Anbieter zur Verfügung gestellte Webserver-Proxy-Plug-in stellt diesen Service bereit.

Verwenden Sie die Verfahren, die für Ihre Bereitstellung zutreffen:

1. Konfigurieren Sie den IBM-HTTP-Server (siehe Seite 315) (Alle Webserver)
2. Konfigurieren Sie das Proxy-Plug-in (siehe Seite 316) (Alle Webserver)
3. Eine der folgenden:
   - Abschließen der Konfiguration auf IIS (siehe Seite 320)
   - Abschließen der Konfiguration auf iPlanet oder Apache (siehe Seite 322)

### Konfigurieren des IBM HTTP-Servers

Für alle Webserver installieren Sie das Proxy-Plug-in und verwenden den Befehl "configurewebserver".

**Gehen Sie wie folgt vor:**

1. Installieren Sie das Proxy-Plug-in von der WebSphere-Startseite.
2. Fügen Sie den Webserver zur WebSphere-Zelle hinzu, indem Sie den Befehl "configurewebserver1.bat" wie folgt ausführen:
   a. Bearbeiten Sie "*websphere_home*\Plugins\bin\configurewebserver1.bat/.sh" in einem Texteditor.
   b. Fügen Sie nach "wsadmin.bat/.sh" einen Benutzernamen und ein Kennwort hinzu, wie folgt:
   ```
   wsadmin.bat -user wsadmin -password Kennwort -f
   configureWebserverDefinition.jacl
   ```
   c. Führen Sie "configurewebserver1.bat/.sh" aus.

   **Hinweis**: Weitere Informationen zum Befehl "configurewebserver" finden Sie in der IBM WebSphere-Dokumentation.
3. Fahren Sie mit dem Vorgang fort, um das Proxy-Plug-in zu konfigurieren (siehe Seite 316).

## Konfigurieren des Proxy-Plug-ins

Für alle Webserver aktualisieren Sie das Plug-in mithilfe des GenPluginCfg-Befehls von WebSphere:

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei dem System an, auf dem WebSphere installiert ist.
2. Navigieren Sie von der Befehlszeile zu "*websphere_home*\bin", wobei *websphere_home* das Installationsverzeichnis von WebSphere ist.

   Beispiel:

   - **Windows:**

     C:\Programme\WebSphere\AppServer\profile\AppSrv01\bin

   - **UNIX:**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin

3. Führen Sie den Befehl "GenPluginCfg.bat" oder "GenPluginCfg.sh" aus.

   Wenn Sie diesen Befehl ausführen, wird die Datei "plugin-cfg.xml" an folgendem Speicherort erstellt:

   *websphere_home*\AppServer\profiles\AppSrv01\config\cells

4. Fahren Sie mit einem der folgenden Vorgänge fort:

   - Abschließen der Konfiguration auf IIS (siehe Seite 320)
   - Abschließen der Konfiguration auf iPlanet oder Apache (siehe Seite 322)

## Abschließen der Konfiguration auf IIS (7.x)

Bevor Sie diesen Vorgang starten, überprüfen Sie, dass Sie eine Version 6.1.0.9 oder höher des Webserver-Plug-ins verwenden. Ältere Plug-in-Versionen unterstützen das Windows Server 2008-Betriebssystem nicht.

**Gehen Sie wie folgt vor:**

1. Installieren Sie IIS-Version 7.x mit den Verwaltungskompatibilitätskomponenten von IIS-Version 6.0. Die Verwaltungskompatibilitätskomponenten von IIS-Version 6.0 werden nicht standardmäßig installiert.
2. Führen Sie die folgenden Schritte aus, um das Server-Manager-Fenster auf Windows Server 2008 aufzurufen:
    1. Klicken Sie auf "Start", "Verwaltung", "Server-Manager".
    2. Klicken Sie auf "Aktion", "Rollen hinzufügen", und klicken Sie dann auf "Weiter".
    3. Wählen Sie die Rolle für Webserver (IIS) auf der Seite "Serverrollen auswählen" aus, und klicken Sie dann auf "Weiter".
    4. Klicken Sie auf "Feature hinzufügen", "Weiter", wenn eine Aufforderung für den Windows-Prozessaktivierungsdienst angezeigt wird.
    5. Klicken Sie auf der IIS-Einführungsseite auf "Weiter".
3. Wenn das Fenster "Rollendienste" angezeigt wird, stellen Sie sicher, dass die folgenden Optionen zusätzlich zu den Standardoptionen, die bereits ausgewählt sind, aktiviert werden.
    - Internet-Informationsdienste: Verwaltungstools
    - IIS-Version 6.0 Management Kompatibilität: IIS-Version 6.0-Management-Konsole, IIS-Version 6.0-Skriptingtools, IIS-Version 6.0-WMI-Kompatibilität und IIS-Metabasiskompatibilität
    - Anwendungsentwicklung: ISAPI-Erweiterungen, ISAPI-Filter
4. Klicken Sie auf "Weiter", um die ausgewählten Optionen zu aktivieren, und dann im nächsten Fenster auf "Installieren" , um die Installation auszuführen.
5. Klicken Sie im Fenster mit dem Installationsergebnis auf "Schließen" , sobald die Installation abgeschlossen ist.
6. Öffnen Sie die Eingabeaufforderung und wechseln Sie zu :\Programme\IBM\WebSphere\AppServer\profiles\Dmgr01\bin.
7. Führen Sie diesen Befehl aus: GenPluginCfg.bat.

    Die plugin-cfg.xml-Datei wird an diesem Speicherort generiert: C:\Programme\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells.
8. Erstellen Sie ein Verzeichnis unter c:\, zum Beispiel "c:\plugin".
9. Kopieren Sie die Datei "plugin-cfg.xml" in das Verzeichnis "c:\plugin".

10. Kopieren Sie "iisWASPlugin_http.dll" in das Verzeichnis "c:\plugin".
11. Klicken Sie auf einem Windows Server 2008 Betriebssystem auf "Start", "Programme", "Verwaltung", "Internet Information Services (IIS) Manager". Diese Aktion startet die IIS-Anwendung und erstellt für die Website-Instanz ein neues virtuelles Verzeichnis. Diese Anweisungen setzen voraus, dass Sie die Standardwebsite verwenden.
12. Erweitern Sie die Struktur auf der linken Seite, bis Sie die Standardwebsite sehen.
13. Klicken Sie mit der rechten Maustaste auf "Standardwebsite", "Virtuelles Verzeichnis hinzufügen", um das Verzeichnis mit einer Standardinstallation zu erstellen.
14. Geben Sie "setPlugins" in das Feld "Alias" im Fenster "Alias für virtuelles Verzeichnis" des Assistenten zum Erstellen virtueller Verzeichnisse ein.
15. Navigieren Sie zum Verzeichnis "c:\plugin" im Feld Physischer Pfad des Assistentenfensters "Verzeichnis des Websiteinhalts", und klicken Sie auf "OK".
16. Klicken Sie auf die angezeigte Schaltfläche, um die Einstellungen zu testen. Wenn der Einstellungstest fehlschlägt, können Sie die Berechtigungen des physischen Verzeichnisses ändern. Wählen Sie alternativ "Verbinden als" aus, und lassen Sie IIS die Verbindung als ein Windows-Benutzerkonto herstellen, das Berechtigungen für die Dateien in diesem physischen Pfad hat.
17. Klicken Sie auf "OK", um das virtuelle Verzeichnis "setPlugins" zu Ihrer Website hinzuzufügen.
18. Wählen Sie das virtuelle Verzeichnis "setPlugins" aus, das Sie gerade in der Navigationsstruktur erstellt haben.
19. Doppelklicken Sie auf "Handlerzuordnungen" und dann im Bereich "Aktionen" auf "Featureberechtigungen bearbeiten".
20. Aktivieren Sie "Skripta" und "Ausführen", wenn diese Optionen nicht bereits ausgewählt sind.
21. Klicken Sie auf "OK".
22. Kehren Sie zum IIS-Manager-Fenster zurück, und blenden Sie den Websites-Ordner in der Navigationsstruktur auf der linken Seite dieses Fensters ein.
23. Wählen Sie in der Navigationsstruktur "Standardwebsite" aus.

24. Führen Sie die folgenden Schritte im Eigenschaftsbereich der Standardwebsite aus, um den ISAPI-Filter hinzuzufügen:
    1. Doppelklicken Sie auf die Registerkarte "ISAPI-Filter".
    2. Klicken Sie, um das Dialogfeld "Filtereigenschaften hinzufügen/bearbeiten" zu öffnen.
    3. Geben Sie "iisWASPlugin" in das Feld "Filtername" ein.
    4. Klicken Sie auf "Durchsuchen", um die Plug-in-Datei im Verzeichnis "c:\plugin\iisWASPlugin_http.dll" auszuwählen.
    5. Klicken Sie auf "OK" , um das Dialogfeld "Filtereigenschaften hinzufügen/bearbeiten" zu schließen.
25. Wählen Sie den obersten Serverknoten in der Navigationsstruktur aus.
26. Doppelklicken Sie im Bereich "Features" auf "ISAPI- und CGI-Einschränkungen".

    Um den anzugebenden Wert der Eigenschaft "ISAPI- oder CGI-Pfad" zu bestimmen, suchen und wählen Sie die gleiche Plug-in-Datei aus, die Sie im vorherigen Schritt ausgewählt haben. Beispiel: "c:\plugin\iisWASPlugin_http.dll".
27. Klicken Sie im Bereich "Aktionen" auf "Hinzufügen".
28. Geben Sie "WASPlugin" im Feld "Beschreibung" ein, aktivieren Sie "Ausführung des Erweiterungspfads zulassen", und klicken Sie dann auf "OK" , um das Dialogfeld "ISAPI- und CGI-Einschränkungen" zu schließen.
29. Erstellen Sie die neue Datei "plugin-cfg.loc" im Verzeichnis "c:\plugin". Legen Sie den Wert in der Datei "plugin-cfg.loc" auf den Speicherort der Konfigurationsdatei fest. Der Standardspeicherort ist "C:\plugin\plugin-cfg.xml".

**Aktualisieren des Web-Agenten**

Nachdem Sie IIS 7.x konfiguriert haben, führen Sie folgende Änderungen im Web-Agenten durch:

1. Klicken Sie auf "Anwendungspools", und ändern Sie den Standardanwendungspool zu klassischem Modus.
2. Klicken Sie auf "Senden".
3. Stellen Sie sicher, dass der Agent in der ISAPI-Filter-Prioritätsliste höher ist als das Plug-in für den Anwendungsserver, der von CA IdentityMinder verwendet wird.
4. Starten Sie IIS-Version 7.x und Ihr WebSphere-Anwendungsserverprofil neu.

## Abschließen der Konfiguration auf IIS

Nachdem Sie den IBM HTTP-Server und das Proxy-Plug-in konfiguriert haben, vergewissern Sie sich, dass "plugin-cfg.xml" des Proxys am richtigen Speicherort ist, und führen Sie die Schritte aus, um eine zusätzliche Plug-in-Datei zu konfigurieren.

**Gehen Sie wie folgt vor:**

1. Kopieren Sie "plugin-cfg.xml" folgendermaßen:
    a. Melden Sie sich beim System an, wo der Web-Agent installiert wird.
    b. Erstellen Sie einen Ordner ohne Leerzeichen auf dem Laufwerk "C:". Beispiel: "C:\plugin".
    c. Kopieren Sie die Datei "plugin-cfg.xml" in den Ordner "C:\plugin".
2. Erstellen Sie eine Datei namens "plugin-cfg.loc" im Ordner "C:\plugin", und fügen Sie die folgende Zeile in die Datei ein:

    C:\plugin\plugin-cfg.xml
3. Laden Sie das Websphere-Plug-in-Installationsprogramm von www.ibm.com auf das System herunter, wo WebSphere installiert ist.
4. Wechseln Sie zum Speicherort des WebSphere-Plug-in-Installationsprogramms.
5. Generieren Sie die Datei "iisWASPlugin_http.dll" durch die Verwendung dieses Befehls:

    ```
    install is:javahome "c:\IBM\WebSphere\AppServer\Java
    ```

    Beantworten Sie auf die angezeigten Fragen basierend auf Ihrer Konfiguration.

    Wenn der Assistent beendet ist, wird die Datei "iisWASPlugin_http.dll" im Ordner "C:\IBM\WebSphere\Plugs\bin" gespeichert. Suchen Sie die Unterordner für 32-Bit oder 64-Bit.
6. Kopieren Sie dieDatei "iisWASPlugin_http.dll" in den Ordner "C:\plugin" auf dem System mit dem Web-Agenten.
7. Erstellen Sie wie folgt ein virtuelles Verzeichnis:
    a. Öffnen Sie den IIS-Manager.
    b. Klicken Sie mit der rechten Maustaste auf die Standardwebsites.
    c. Klicken Sie auf "Neues virtuelles Verzeichnis" und geben Sie diese Werte an:

        Alias: sePlugins (es Groß- und Kleinschreibung beachtet wird)

        Pfad: c:\plugin

        Berechtigung: Lesen + Ausführen (ISAPI oder CGI)

8. Fügen Sie wie folgt einen ISAPI-Filter hinzu:
   a. Klicken Sie mit der rechten Maustaste auf die Standardwebsite.
   b. Klicken Sie auf "Eigenschaften".
   c. Klicken Sie auf der Registerkarte "ISAPI-Filter" auf "Hinzufügen".
   d. Geben Sie diese Werte an:

      Filtername: sePlugins

      Ausführbar: c:\plugin\ iisWASPlugin_http.dll
9. Erstellen Sie wie folgt eine Webdiensterweiterung:
   a. Blenden Sie in IIS6 Manager den Computernamen ein.
   b. Erstellen Sie eine Webdiensterweiterung, und setzen Sie sie auf "Zulassen".

      Erweiterungsname: WASPlugin

      Pfad: C:\plugin\ iisWASPlugin_http.dll
   c. Klicken Sie mit der rechten Maustaste auf jede Webdiensterweiterung, um sie zum Status "Zugelassen" zu ändern.
10. Starten Sie den IIS Webserver neu.

    Stellen Sie im Master-WWW-Service sicher, dass das WebSphere-Plug-in (sePlugin) nach dem SiteMinder-Web-Agent-Plug-in angezeigt wird und dass das WebSphere-Plug-in erfolgreich gestartet wurde.

## Abschließen der Konfiguration auf iPlanet oder Apache

Nachdem Sie den IBM HTTP-Server und das Proxy-Plug-in konfiguriert haben, vergewissern Sie sich, dass "plugin-cfg.xml" des Proxys am richtigen Speicherort ist und starten den Webserver neu.

**Gehen Sie wie folgt vor:**

1. Kopieren Sie "plugin-cfg.xml" aus dem System, wo Sie das Proxy-Plug-in installiert haben, zum folgenden Speicherort:

   *websphere_home*\AppServer\profiles*server_name*\config\cells*websphere_cell*\nodes\webserver1_node\servers\webserver1\

2. Stellen Sie sicher, dass das WebSphere-Plug-in (libns41_http.so) nach dem SiteMinder-Web-Agent-Plug-in (NSAPIWebAgent.so) auf allen iPlanet-Webservern geladen wird.

3. Überprüfen Sie die Reihenfolge von Plug-ins in "*iplanet_home*/https-*instance*/config/magnus.conf" für IPlanet-6.0-Webserver.

4. Kopieren Sie die folgenden Zeilen von "*iplanet_home*/https-*instance*/config/magnus.conf" nach "*iplanet_home*/https-*instance*/config/obj.conf" (IPlanet-5.x-Webserver):

   Init fn="load-modules" funcs="as_init,as_handler,as_term" shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init" bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"

   Fügen Sie nach AuthTrans fn="SiteMinderAgent" in der obj.conf-Datei den folgenden Code hinzu:

   Service fn="as_handler"

5. Stellen Sie sicher, dass das SiteMinder-Web-Agent-Plug-in (mod2_sm.so) auf Apache-Webservern vor dem WebSphere-Plug-in (mod_ibm_app_server_http.so) geladen wird. Dieser Befehl befindet sich im Abschnitt Dynamic Shared Object (DSO) Support von *apache_home*/config/httpd.conf,

6. Starten Sie den Webserver neu.

## Installieren Sie das Proxy-Plug-in für JBoss.

Nachdem der SiteMinder-Web-Agent eine Anfrage für eine CA IdentityMinder-Ressource authentifiziert und genehmigt hat, leitet der Webserver die Anfrage an den Anwendungsserver weiter, der den CA IdentityMinder-Server hostet. Um diese Anfragen weiterzuleiten, installieren und konfigurieren Sie einen JK-Connector auf dem System, wo der SiteMinder-Web-Agent installiert ist. Weitere Informationen zum JK-Connector finden Sie auf der Jakarta Projektwebsite:

http://community.jboss.org/wiki/usingmodjk12withjboss

Die CA IdentityMinder-Verwaltungstools schließen Beispielkonfigurationsdateien ein, die Sie verwenden können, um den JK-Connector zu konfigurieren. Anweisungen finden Sie in der readme.txt-Datei in dem in der folgenden Tabelle angegebenen Verzeichnis:

| Plattform | Standort |
|---|---|
| IIS-Webserver auf einem Windows-System | C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss* |
| Sun Java-System-Webserver auf einem Solaris-System | /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss* |
| Apache-Webserver auf einem Solaris-System | /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss* |

### Installieren und Konfigurieren eines JBoss-Anwendungs-Plug-ins (IIS 7.x)

Dieser Vorgang beschreibt die Konfiguration des JBoss-Apache-Plug-ins ab IIS 7.0

Gehen Sie wie folgt vor:

1. Stellen Sie ISAPI-Filter auf dem Dateisystem bereit und aktualisieren Sie sie.

   Stellen Sie den ISAPI-Ordner im Stammverzeichnis des Laufwerks C bereit.

2. Bearbeiten Sie die Datei "jakarta.reg" im entpackten Ordner.

   Wenn Sie den ISAPI-Ordner im Stammverzeichnis von C:\ platziert haben, ändern Sie diese Datei nicht. Wenn Sie sie in einem anderen Ordner abgelegt haben, geben Sie diesen Ordner in den Zeilen 9, 11 und 12 an.

3. Speichern Sie Ihre Änderungen und doppelklicken Sie dann, um die Registrierung zu aktualisieren.

4. Bearbeiten Sie die Datei "workers.properties" durch das Angeben des Speicherorts Ihres JBoss-Anwendungsservers. Der Port und Typ müssen nicht geändert werden.

5. Installieren Sie IIS7 oder IIS7.5 unter Windows 2008.

6. Öffnen Sie den Systemmanager und überprüfen Sie, dass IIS-ISAPI-Filter und ISAPI-Erweiterung installiert sind.
7. Starten Sie "inetmgr" im Fenster "Ausführen".
8. Wählen Sie den Namen aus und doppelklicken Sie auf "ISAPI- und CGI-Einschränkungen".
9. Klicken Sie auf der rechten Seite auf "Hinzufügen".
10. Das Fenster "ISAPI- und CGI-Einschränkungen hinzufügen" wird angezeigt.
11. Wählen Sie "isapi_redirect.dll" aus, und geben Sie als Beschreibung ISAPI ein.
12. Aktivieren Sie das Kontrollkästchen "Ausführung des Erweiterungspfads zulassen".
13. Klicken Sie im Fenster "ISAPI- und CGI-Einschränkungen hinzufügen" auf "OK".
14. Erweitern Sie im Bereich "Verbindungen" den Knoten "Sites", wählen Sie die Standardwebsite aus, und klicken Sie mit der rechten Maustaste auf "Virtuelles Verzeichnis hinzufügen".
15. Geben Sie als Alias "jakarta" ein, und geben Sie den Speicherort der Datei "isap_redirect.dll" (c:\ajp) in den physischen Pfad ein.
16. Klicken Sie auf die Schaltfläche "Einstellungen testen":
    - Wenn Authentifizierung und Autorisierung bestanden wurden, klicken Sie auf "OK".
    - Wenn die Autorisierung fehlschlägt, klicken Sie auf die Schaltfläche "Verbinden als".
17. Wählen Sie "Bestimmter Benutzer" aus, und geben Sie den Admin-Benutzernamen und das Kennwort an.
18. Klicken Sie erneut auf die Schaltfläche "Einstellungen testen". Diesmal funktioniert die Autorisierung.
19. Klicken Sie auf die Standardwebsite auf der linken Seite, und doppelklicken Sie auf den ISAPI-Filter klicken.
20. Klicken Sie auf der rechten Seite auf "Hinzufügen".
21. Geben Sie den Namen ein, und geben Sie den Speicherort der Datei "isapi_redirect.dll" an.
22. Klicken Sie auf "OK".
23. Blenden Sie die Standardwebsiet ein, und klicken Sie auf das virtuelle Jakarta-Verzeichnis.
24. Doppelklicken Sie auf "Handlerzuordnung".
25. Wählen Sie "ISAPI-dll" aus, und klicken Sie auf "Featureberechtigungen bearbeiten".

26. Überprüfen Sie, dass alle Berechtigungen (Lesen, Skripts, Ausführen) aktiviert sind.
27. Klicken Sie auf "OK".

**Aktualisieren des Web-Agenten**

Nachdem Sie IIS 7.x konfiguriert haben, führen Sie folgende Änderungen im Web-Agenten durch:

1. Klicken Sie auf "Anwendungspools", und ändern Sie den Standardanwendungspool zu klassischem Modus.
2. Klicken Sie auf "Senden".
3. Stellen Sie sicher, dass der Agent in der ISAPI-Filter-Prioritätsliste höher ist als das Plug-in für den Anwendungsserver, der von CA IdentityMinder verwendet wird.

Das JBoss-Plug-in wird konfiguriert.

## Installieren und Konfigurieren eines JBoss-Anwendungs-Plug-ins (IIS 6.0)

Diese Integration setzt voraus, dass SiteMinder einen Benutzer authentifiziert und genehmigt, bevor es CA IdentityMinder erreicht. Ein Benutzer muss einen SMSESSION-Cookie haben, bevor er CA IdentityMinder erreicht. Verwenden Sie ein von einem SiteMinder-Web-Agenten geschütztes Anwendungs-Plug-in (Proxy-Umleitung). Durch diese Konfiguration wird ein Benutzer von SiteMinder authentifiziert und dann an CA IdentityMinder umgeleitet, nachdem ein SMSESSION-Cookie erstellt worden ist.

Dieses Verfahren gilt für die Bereitstellung und Konfiguration des JBoss-Apache-Plug-ins für IIS 6.0:

**Gehen Sie wie folgt vor:**

1. Stellen Sie einen ISAPI-Filter auf dem Dateisystem bereit und aktualisieren Sie ihn.

   Stellen Sie den ISAPI-Ordner im Stammverzeichnis des Laufwerks C bereit.
2. Bearbeiten Sie die Datei "jakarta.reg" im entpackten Ordner.

   Wenn Sie den ISAPI-Ordner im Stammverzeichnis von C:\ platziert haben, ändern Sie diese Datei nicht. Wenn Sie sie in einem anderen Ordner ablegen, geben Sie diesen Ordner in den Zeilen 9, 11 und 12 an.
3. Speichern Sie Ihre Änderungen und doppelklicken Sie dann, um die Registrierung zu aktualisieren.
4. Bearbeiten Sie die Datei "workers.properties" durch das Angeben des Speicherorts Ihres JBoss-Anwendungsservers. Der Port und Typ müssen nicht geändert werden.
5. Stellen Sie den ISAPI-Filter auf IIS bereit.
6. Öffnen Sie den Internetinformationsdienste-Manager über die Verwaltung.
7. Blenden Sie die Ebenen ein, bis die Standardwebsite sichtbar ist. Klicken Sie mit der rechten Maustaste, und wählen Sie "Neu", "Virtuelles Verzeichnis" aus.

8. Geben Sie *jakarta* als Alias ein.
9. Verweisen Sie auf den Pfad, wo Sie das ISAPI-Plug-in installiert haben.
10. Aktivieren Sie "Lesen", "Skripts ausführen" (wie ASP) und "Ausführen" (wie ISAPI-Anwendungen oder CGI).
11. Klicken Sie auf "Weiter", um fortzufahren und den Assistenten fertig zu stellen.
12. Klicken Sie mit der rechten Maustaste auf "Standardwebsites", und wählen Sie "Eigenschaften" aus. Wählen Sie die Registerkarte "ISAPI-Filter" aus, und klicken Sie auf "Hinzufügen".
13. Geben Sie *jakarta* für den Filternamen ein, und klicken Sie dann auf "Durchsuchen", um "isapi_redirect.dll" auszuwählen. Klicken Sie anschließend zweimal auf "OK".
14. Aktivieren Sie für IIS 6.0 diesen Filter unter den Webdiensterweiterungen.
15. Wählen Sie den Webdiensterweiterungs-Ordner aus. Klicken Sie auf den blauen Link links für "Neue Webdiensterweiterung hinzufügen".
16. Geben Sie "Jakarta-Tomcat" als Name an. Klicken Sie auf "Hinzufügen", und suchen Sie die gleiche dll wie oben. Klicken Sie auf "OK". Aktivieren Sie "Erweiterungsstatus auf 'Zugelassen' setzen", und klicken Sie dann auf "OK".
17. Starten Sie den IIS Server neu.

Mit dem jetzt eingerichteten Proxy können Sie über IIS auf CA IdentityMinder zugreifen. Hier sind beispielsweise die Links, um auf CA IdentityMinder zuzugreifen, vor und nach der Proxy-Konfiguration:

**Vor**

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

**Nach**

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

**Hinweis:** Ein Schrägstrich "/" kann am Ende dieser URL gebraucht werden, damit der Proxy arbeitet. Überprüfen Sie die Proxy-Protokolle, wenn Sie nicht zur Management-Konsole weitergeleitet werden.

## Installieren des Proxy-Plug-ins auf WebLogic

Sobald der Web-Agent eine Anfrage für eine CA IdentityMinder-Ressource authentifiziert und genehmigt hat, leitet der Webserver die Anfrage an den Anwendungsserver weiter, der den CA IdentityMinder-Server hostet.

1. Installieren Sie das WebLogic-Proxy-Plug-in für Ihren Webserver, wie in der WebLogic-Dokumentation beschrieben.

   **Hinweis:** Wenn Sie das Proxy-Plug-in als IIS-Benutzer installieren, konfigurieren Sie die Proxy-Weiterleitung nach Dateierweiterung und Pfad. Wenn Sie die Proxy-Weiterleitung nach Dateierweiterung konfigurieren, fügen Sie eine Anwendungszuordnung in der Registerkarte "Anwendungszuordnung" mit den folgenden Eigenschaften hinzu:
   **Ausführbare Datei:** IISProxy.dll
   **Erweiterung:** .wlforward

2. Konfigurieren Sie das Proxy-Plug-in für CA IdentityMinder, wie in einem der folgenden Abschnitte beschrieben:

   - Proxy-Plug-in für IIS (siehe Seite 330)
   - Proxy-Plug-in für iPlanet (siehe Seite 331)
   - Proxy-Plug-in für Apache (siehe Seite 334)

### Konfigurieren des Proxy-Plug-Ins für IIS (7.x)

Folgender Vorgang durchläuft die Bereitstellung und Konfiguration des WebLogic-Proxy-Plug-ins für IIS 7.x.

**Hinweis:** Diese Anweisungen sind für 32-Bit-Umgebungen. Die gleichen Anweisungen gelten für 64-Bit-Umgebungen. Der Speicherort der .dll-Installationsdatei ist unterschiedlich:

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

Gehen Sie wie folgt vor:

1. Installieren Sie den Web-Agent auf IIS7 und konfigurieren ihn.
2. Erstellen Sie einen Ordner mit dem Namen "plugin" auf dem Laufwerk C.
3. Kopieren Sie die folgenden Dateien zum Ordner "plugin":

   - Iisforward.dll
   - Iisproxy.dll
   - iisproxy.ini

   Sie finden diese Dateien unter "\\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7".

4. Installieren Sie die Anwendungsentwicklungs- und Verwaltungstools-Rollendienste auf IIS7.
5. Öffnen Sie Inet Manager, und wählen Sie die Standardwebsite aus.
6. Klicken Sie auf "Handlerzuordnungen".
7. Doppelklicken Sie auf "Statische Datei", und ändern Sie den Anforderungspfad in *.*.
8. Klicken Sie auf die Schaltfläche "Einschränkungen".
9. Aktivieren Sie auf der Registerkarte "Zuordnung" die Option "Handler nur bei folgender Zuordnung aufrufen" "Datei oder Ordner".
10. Klicken Sie im Dialogfeld "Handlerzuordnungen" in den Menüoptionen auf der rechten Seite auf "Skriptzuordnung hinzufügen". Geben Sie die folgenden Werte ein:
    - Anforderungspfad : *
    - Ausführbare Datei: iisProxy.dll
    - Name: proxy
11. Klicken Sie auf die Schaltfläche "Einschränkungen".
12. Deaktivieren Sie die Option "Handler nur bei folgender Zuordnung aufrufen".
13. Klicken Sie in der Eingabeaufforderung, ob diese IASPI-Erweiterung erlaubt werden soll, auf "Ja".
14. Klicken Sie auf den Stammknoten (Computername) der IIS-Manager-Struktur, und klicken Sie auf "ISAPI- und CGI-Einschränkungen".
15. Klicken Sie im Bereich "Aktionen" auf "Hinzufügen", und geben Sie die folgenden Werte ein:
    - ISAPI- oder CGI-Pfad: C:\plugin\ iisproxy.dll
    - Beschreibung: Weblogic
    - Aktivieren Sie das Kontrollkästchen "Ausführung des Erweiterungspfads zulassen".
16. Klicken Sie auf den Stammknoten (Computername) der IIS-Manager-Struktur, und klicken Sie auf "ISAPI- und CGI-Einschränkungen". Wählen Sie die Option "Weblogic" aus, und klicken Sie auf der rechten Seite auf "Featureberechtigungen bearbeiten".
17. Aktivieren Sie "Nicht angegebene ISAPI-Module zulassen" und "Nicht angegebene CGI-Module zulassen".
18. Machen Sie das Gleiche für Web-Agent.
19. Doppelklicken Sie in der Ansicht " Features" der Standardwebsite auf "Handlerzuordnungen".

20. Klicken Sie auf der Seite "Handlerzuordnungen", im Bereich "Aktionen" auf "Skriptzuordnung hinzufügen", und fügen Sie die folgenden Werte hinzu:
    - Anforderungspfad: .jsp
    - Ausführbare Datei: iisproxy.dll
    - Name: JSP
21. Klicken Sie auf "Einschränkungen".
22. Aktivieren Sie auf der Registerkarte "Zuordnung" die Option "Handler nur bei folgender Zuordnung aufrufen" "Datei".
23. Klicken Sie auf "OK".
24. Klicken Sie auf "Skriptzuordnung hinzufügen", und fügen Sie die folgenden Werte hinzu:
    - Anforderungspfad: .do
    - Ausführbare Datei: C:\plugin\iisproxy.dll
25. Klicken Sie auf "Einschränkungen". Die Einstellungen sind die gleichen wie .jsp.
26. Klicken Sie auf "OK".
27. Klicken Sie auf "Skriptzuordnung hinzufügen", und geben Sie die folgenden Werte ein:
    - Anforderungspfad:  .wlforward
    - Ausführbare Datei: C:\plugin\iisproxy.dll
28. Klicken Sie auf "Einschränkungen". Die Einstellungen sind die gleichen wie für .jsp.
29. Klicken Sie auf "Standardwebsite", und doppelklicken Sie auf "ISAPI-Filter".
30. Klicken Sie auf der rechten Seite auf "Sortierte Liste anzeigen".
31. Platzieren Sie die ausführbare Datei des SiteMinder-Agent an zweiter Stelle in der Liste. Nach diesem Eintrag befindet sich nur noch die ausführbare Weblogic-Datei in der Liste.

    **Hinweis**: Wenn die ausführbare Datei des SiteMinder-Agent nach der ausführbaren Weblogic-Datei angezeigt wird, dann verschieben Sie den SiteMinder-Agenten mithilfe des Pfeils "Nach oben".
32. Klicken Sie auf "Anwendungspools", und ändern Sie den Standardanwendungspool zu klassischem Modus.

Das WebLogic-Plug-in ist konfiguriert.

## Konfigurieren des IIS 6.0 Proxy-Plug-ins

Diese Vorgehensweise bezieht sich auf Konfigurationen des WebLogic-Proxy-Plug-ins für IIS 6.0.x:

**Gehen Sie wie folgt vor:**

1. Erstellen Sie einen Ordner auf dem System, wo der Web-Agent installiert ist. Beispiel: "c:\weblogic_proxy".
2. Melden Sie sich beim System an, wo der CA IdentityMinder-Server ausgeführt wird.
3. Wechseln Sie zu diesem Ordner: *Weblogic_Home*\wlserver_11\server\plugin
4. Kopieren Sie die folgenden Dateien zu dem in Schritt 1 erstellten WebLogic-Proxy-Ordner.
   - iisforward.dll
   - iisproxy.dll
5. Erstellen Sie eine Datei namens "iisproxy.ini" im gleichen Ordner, und geben Sie den folgenden Inhalt ein:

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=host-name
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im
   WLLogFile= c:\weblogic_proxy \proxy.log
   DebugConfigInfo=ON
   ```

   Ersetzen Sie *host-name* durch den eigentlichen Hostnamen.
6. Starten Sie IIS Manager.
7. Erweitern Sie die Websites.
8. Klicken Sie mit der rechten Maustaste auf die Standardwebsite.
9. Wählen Sie "Eigenschaften" aus.
10. Fügen Sie wie folgt einen Filter hinzu:
    a. Klicken Sie auf "host-name".
    b. Klicken Sie auf "Hinzufügen", und füllen Sie das Dialogfeld folgendermaßen aus:

       Filtername: WebLogic

       Ausführbare Datei: Pfad von iisforward.dll

11. Geben Sie den Speicherort der iisproxy.dll-Datei wie folgt an:
    a. Klicken Sie auf "Basisverzeichnis".
    b. Klicken Sie auf "Konfiguration".
    c. Klicken Sie auf "Hinzufügen".
    d. Geben Sie den Pfad der iisproxy.dll-Datei ein.
    e. Geben Sie ".jsp" in das Feld "Erweiterung" ein.
    f. Deaktivieren Sie die Option "Verifizieren, dass Datei existiert".
12. Wiederholen Sie Schritt 11 für die Erweiterungen ".do" und ".wlforward".
13. Fügen Sie eine Webdiensterweiterung für "wlforward" hinzu (kleingeschrieben), die auf den Speicherort von "iisforward.dll" verweist.

    Legen Sie den Erweiterungsstatus auf "Zugelassen" fest.
14. Klicken Sie mit der rechten Maustaste auf jede Webdiensterweiterung, um sie zum Status "Zugelassen" zu ändern.
15. Starten Sie den IIS Webserver neu.

## Konfigurieren des Proxy-Plug-ins für iPlanet

Um das Plug-in zu konfigurieren, ändern Sie die folgenden iPlanet-Konfigurationsdateien:

- magnus.conf
- obj.conf

Die iPlanet-Konfigurationsdateien haben strikte Regeln über die Textposition. Um Probleme zu vermeiden, beachten Sie die folgenden Punkte:

- Entfernen Sie zusätzliche führende und nachgestellte Leerzeichen. Zusätzliche Leerzeichen können dazu führen, dass Ihr iPlanet-Server fehlschlägt.
- Wenn Sie mehr Zeichen eingeben müssen, als auf eine Zeile passen, geben Sie einen umgekehrten Schrägstrich (\) am Ende dieser Zeile ein und fahren auf der folgenden Zeile mit der Eingabe fort. Der umgekehrte Schrägstrich wird direkt zwischen dem Ende der ersten Zeile und dem Anfang der folgenden Zeile eingefügt. Wenn ein Leerzeichen zwischen den Wörtern am Ende der ersten Zeile und dem Beginn der zweiten Zeile notwendig ist, geben Sie entweder am Ende der ersten Zeile (vor dem umgekehrten Schrägstrich) oder am Anfang der zweiten Zeile ein Leerzeichen ein.
- Teilen Sie keine Attribute über mehreren Zeilen.

Die iPlanet-Konfigurationsdateien für Ihre iPlanet-Instanz befinden sich an folgendem Speicherort:

*iplanet_home*/https-*instance_name*/config/

wobei *iplanet_home* das Stammverzeichnis der iPlanet-Installation und *instance_name* Ihre jeweilige Serverkonfiguration ist.

**Gehen Sie wie folgt vor:**

1. Kopieren Sie aus dem Verzeichnis "*weblogic_home/server*/lib" die Datei "libproxy.so", die Ihrer Version des iPlanet-Webservers auf dem Dateisystem entspricht, wo Sie iPlanet installiert haben.
2. Ändern Sie in einem Texteditor die iPlanet-Datei "magnus.conf".

   Um iPlanet anzuweisen, die Datei "libproxy.so" als ein iPlanet-Modul zu laden, fügen Sie die folgenden Zeilen am Anfang der magnus.conf-Datei hinzu:
   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=Pfad in Dateisystem aus Schritt 1/libproxy.so
   Init fn="wl_init"
   ```
   Beispiel:
   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```
   Das Funktionslademodul kennzeichnet die gemeinsam genutzte Bibliothek zum Laden, wenn iPlanet startet. Die Werte "wl_proxy" und "wl_init" identifizieren die Funktionen, die das Plug-in ausführt.

3. Ändern Sie in einem Texteditor die iPlanet-Datei "obj.conf" wie folgt:

   a. Nach der letzten Zeile, die mit dem folgenden Text anfängt:

      NameTrans fn=....

      Fügen Sie die folgende Service-Direktive zum Abschnitt für Object name="default" hinzu:

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      **Hinweis:** Sie können diese Direktive in einer Zeile nach den vorhanden Service-Direktiven hinzufügen.

   b. Fügen Sie den folgenden Code am Ende der Datei hinzu:

      ```
      <Object name="idm" ppath="*/iam/*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      wobei *Hostname* der Servername und die Domäne des Systems ist, wo Sie WebLogic installiert haben, und *portnumber* der WebLogic-Port ist (Standard ist 7001).

      Sie können mehr als einen Object-Eintrag haben.

      Beispiel:

      ```
      <Object name="idm" ppath="*/iam/*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. Speichern Sie die iPlanet-Konfigurationsdatei.

5. Starten Sie Ihre Webserver-Instanz neu.

## Konfigurieren des Proxy-Plug-ins für Apache

Das Konfigurieren des Apache-Proxy-Plug-ins bearbeiten Sie die Datei "http.conf".

**Gehen Sie wie folgt vor:**

1. Halten Sie den Apache-Webserver an, nachdem Sie einen Web-Agenten unter Solaris installiert haben, und kopieren Sie die Datei "mod_wl_20.so" vom folgenden Speicherort:

   *weblogic_home*/server/lib/solaris

   in

   *apache_home*/modules

2. Bearbeiten Sie die Datei "http.conf" (unter *apache_home/conf*), und nehmen Sie die folgenden Änderungen vor:

   a. Fügen Sie unter dem Lademodulabschnitt den folgenden Code hinzu:
   ```
   LoadModule weblogic_module     modules/mod_wl_20.so
   ```

   b. Bearbeiten Sie den Servernamen mit dem Namen des Apache-Serversystems.

   c. Fügen Sie einen If-Block am Ende der Datei hinzu, wie folgt:
   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
   </IfModule>
   ```

3. Speichern Sie die Datei "http.conf".

4. Starten Sie den Apache-Webserver neu.

# Ordnen Sie den SiteMinder-Agenten einer CA IdentityMinder-Domäne zu

Der Richtlinienadministrator führt diese Aufgabe aus, nachdem er die CA IdentityMinder-Aufgaben abgeschlossen hat. Während Sie Ihre Umgebungen in CA IdentityMinder laden, verweisen Sie auf den 4.X-Agenten. SiteMinder verwendet diesen Agenten, wenn er die Domäne bzw. den Bereich auf dem SiteMinder-Richtlinienserver erstellt. Dieser Agent validiert SMSESSION-Cookies. Aktualisieren Sie die Domäne bzw. den Bereich, und verweisen Sie auf den voll funktionsfähigen Agenten, der sich auf dem Webserver befindet und verwendet wird, um auf CA IdentityMinder zuzugreifen. Dieser Webserver handelt als Zugriffspunkt für CA IdentityMinder und erstellt SMSESSION-Cookies.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich auf der SiteMinder-Verwaltungsoberfläche an.
2. Navigieren Sie zu "Richtlinien", "Domänen".
3. Ändern Sie die Domäne für Ihre Umgebung.
4. Bearbeiten Sie auf der Registerkarte "Bereiche" den ersten aufgelisteten Bereich: XXX_ims_realm.
5. Suchen Sie und wählen Sie den Agenten auf Ihrem Proxy aus.

   **Hinweis:** Wenn Sie keinen Proxy-Agenten (Webserver-Agent) haben, erstellen Sie einen. Überprüfen Sie, dass Sie einen Webserver und einen Proxy an Ort und Stelle vor CA IdentityMinder haben.
6. Klicken Sie zweimal auf "OK" und wiederholen Sie dann diesen Prozess für den öffentlichen Bereich "XXX_pub_realm".
7. Nachdem Sie beide Bereiche aktualisiert haben, klicken Sie auf "Senden".
8. Warten Sie auf die Aktualisierung des Agenten, oder starten Sie den Webserver neu, wo sich der Proxy-Agent befindet.

# Konfigurieren des SiteMinder-Parameters "LogOffUrI"

Nachdem Sie SiteMinder zur Umgebung hinzugefügt haben, bewirkt das Abmelden in CA IdentityMinder eigentlich nichts. Um diese Funktionalität wieder zu aktivieren, aktualisieren Sie das Agent-Konfigurationsobjekt (ACO) für den Agenten auf dem Proxy.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich auf der SiteMinder-Verwaltungsoberfläche an. Klicken Sie auf die Registerkarte "Infrastruktur", erweitern Sie "Agent-Konfiguration", und klicken Sie dann auf "Agent-Konfiguration ändern".
2. Suchen Sie Ihr ACO. Suchen Sie den Parameter "#LogoffUri". Klicken Sie auf die Wiedergabeschaltfläche (nach rechts gerichteter Pfeil) links von diesem Parameter.
3. Entfernen Sie das Rautenzeichen (#) aus dem Namen im Feld "Wert", und geben Sie "/idm/logout.jsp" ein.
4. Klicken Sie auf "OK" und dann "Senden", um das Agent-Konfigurationsobjekt zu aktualisieren.

   Wenn der Agent das nächste Mal seine Konfiguration aus dem Richtlinienserver abruft, wird die neue Einstellung übertragen.

# Fehlerbehebung

Die folgenden Themen beschreiben häufige Fehler, die auftreten können. Wo eine Behebung möglich ist, wurde diese zusammen mit dem Fehler angegeben, um Ihnen bei der Integration zu helfen.

## Fehlende Windows-DLL

**Symptom:**

Fehlende Windows-DLL (MSVCP71.dll)

Wir haben festgestellt, dass JBoss nach der Aktivierung der SiteMinder-Verbindung einen Java-Fehler über eine fehlende DLL auslöst (MSVCP71.dll).

**Hinweis:** Dieser Fehler wird möglicherweise nicht angezeigt, wenn JBoss als Dienst ausgeführt wird. Wenn möglich, testen Sie Ihre Konfiguration, ohne JBoss als Dienst auszuführen.

Lösung:

Gehen Sie wie folgt vor:

1. Suchen Sie MSVCP71.dll auf dem SiteMinder-Richtlinienserver, wenn es unter Windows läuft.
2. Kopieren Sie diese DLL (MSVCP71.dll) in den Ordner "\Windows\system32".
3. Nachdem Sie diese Datei am richtigen Speicherort platziert haben, registrieren Sie sie beim BS.
4. Führen Sie von einem Befehlsfenster den regsvr32-Befehl aus. Solange die Datei geladen ist, sollte alles in Ordnung sein.
5. Starten Sie den Anwendungsserver neu.

## Falscher SiteMinder-Richtlinienserver-Speicherort

**Symptom:**

Falscher SiteMinder-Richtlinienserver-Speicherort.

**Lösung:**

Wird ein falscher Speicherort angegeben, wird in "ra.xml" der Fehler "Cannot connect to policy server: xxx" in der folgenden Abbildung dargestellt angezeigt:

```
2010-12-13 10:26:23,293 WARN  [ims.default] ################################################
2010-12-13 10:26:23,293 WARN  [ims.default] ################################################
2010-12-13 10:26:23,293 WARN  [ims.default] # CA Identity Manager 12.5.4.0.461
2010-12-13 10:26:23,293 WARN  [ims.default] ################################################
2010-12-13 10:26:23,293 WARN  [ims.default] ---- CA IAM FW Startup Sequence Initiated. ----
2010-12-13 10:26:23,293 WARN  [ims.default] * Startup Step 1 : Attempting to start ServiceLocator.
2010-12-13 10:26:23,465 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Task Persistence is up to date.
2010-12-13 10:26:23,497 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Archive is up to date.
2010-12-13 10:26:23,528 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Auditing is up to date.
2010-12-13 10:26:23,559 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Report Snapshot is up to date.
2010-12-13 10:26:23,559 WARN  [ims.default] * Startup Step 2 : Attempting to start PolicyServerService
2010-12-13 10:26:25,809 WARN  [org.jboss.resource.connectionmanager.JBossManagedConnectionPool] Throwable while attempting to get a new
connection: null
javax.resource.spi.EISSystemException: Cannot connect to policy server: dfsadf: dfsadf
      at com.netegrity.ra.policyserver.impl.PSManagedConnectionFactory.createManagedConnection(PSManagedConnectionFactory.java:299)
      at org.jboss.resource.connectionmanager.InternalManagedConnectionPool.createConnectionEventListener
(InternalManagedConnectionPool.java:619)
      at org.jboss.resource.connectionmanager.InternalManagedConnectionPool.getConnection(InternalManagedConnectionPool.java:264)
      at org.jboss.resource.connectionmanager.JBossManagedConnectionPool$BasePool.getConnection(JBossManagedConnectionPool.java:575)
      at org.jboss.resource.connectionmanager.BaseConnectionManager2.getManagedConnection(BaseConnectionManager2.java:347)
      at org.jboss.resource.connectionmanager.TxConnectionManager.getManagedConnection(TxConnectionManager.java:330)
      at org.jboss.resource.connectionmanager.BaseConnectionManager2.allocateConnection(BaseConnectionManager2.java:402)
      at org.jboss.resource.connectionmanager.BaseConnectionManager2$ConnectionManagerProxy.allocateConnection
(BaseConnectionManager2.java:849)
```

**Gehen Sie wie folgt vor:**

1. Überprüfen Sie den in "ra.xml" angegebenen Hostnamen.

```
</config-property>
<config-property>
    <config-property-name>ConnectionURL</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>smserver.forwardinc.ca,44441,44442,44443</config-property-value>
</config-property>
<config-property>
    <config-property-name>UserName</config-property-name>
```

2. Geben Sie in der Eigenschaft "ConnectionURL" Ihren SiteMinder-Richtlinienserver-Hostnamen an. Verwenden Sie einen voll qualifizierten Namen (FQN).

## Falscher Admin-Name

**Symptom:**

Falscher Admin-Name

**Lösung:**

Wird ein falscher Admin angegeben, wird in "ra.xml" der Fehler "Unknown administrator" wie in der folgenden Abbildung dargestellt angezeigt:

```
2010-12-13 10:31:23,653 WARN  [ims.default] ################################################
2010-12-13 10:31:23,653 WARN  [ims.default] # IAM Framework 12.5.4.0.461
2010-12-13 10:31:23,653 WARN  [ims.default] ################################################
2010-12-13 10:31:23,653 WARN  [ims.default] ################################################
2010-12-13 10:31:23,653 WARN  [ims.default] # CA Identity Manager 12.5.4.0.461
2010-12-13 10:31:23,653 WARN  [ims.default] ################################################
2010-12-13 10:31:23,653 WARN  [ims.default] ---- CA IAM FW Startup Sequence Initiated. ----
2010-12-13 10:31:23,653 WARN  [ims.default] * Startup Step 1 : Attempting to start ServiceLocator.
2010-12-13 10:31:23,809 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Task Persistence is up to date.
2010-12-13 10:31:23,840 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Archive is up to date.
2010-12-13 10:31:23,887 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Auditing is up to date.
2010-12-13 10:31:23,981 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Report Snapshot is up to date.
2010-12-13 10:31:23,981 WARN  [ims.default] * Startup Step 2 : Attempting to start PolicyServerService
2010-12-13 10:31:25,262 WARN  [org.jboss.resource.connectionmanager.JBossManagedConnectionPool] Throwable while
attempting to get a new connection: null
javax.resource.spi.EISSystemException: Cannot connect to policy server: Unknown administrator
	at com.netegrity.ra.policyserver.impl.PSManagedConnectionFactory.createManagedConnection
(PSManagedConnectionFactory.java:299)
	at org.jboss.resource.connectionmanager.InternalManagedConnectionPool.createConnectionEventListener
(InternalManagedConnectionPool.java:619)
	at org.jboss.resource.connectionmanager.InternalManagedConnectionPool.getConnection
(InternalManagedConnectionPool.java:264)
	at org.jboss.resource.connectionmanager.JBossManagedConnectionPool$BasePool.getConnection
(JBossManagedConnectionPool.java:575)
	at org.jboss.resource.connectionmanager.BaseConnectionManager2.getManagedConnection
(BaseConnectionManager2.java:347)
	at org.jboss.resource.connectionmanager.TxConnectionManager.getManagedConnection(TxConnectionManager.java:330)
	at org.jboss.resource.connectionmanager.BaseConnectionManager2.allocateConnection
(BaseConnectionManager2.java:402)
	at org.jboss.resource.connectionmanager.BaseConnectionManager2$ConnectionManagerProxy.allocateConnection
(BaseConnectionManager2.java:849)
```

**Gehen Sie wie folgt vor:**

1. Überprüfen Sie die Eigenschaft "UserName" in "ra.xml".

```
    <config-property-value>smserver.forwardinc.ca,44441,44442,44443</co
</config-property>
<config-property>
    <config-property-name>UserName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>SiteMinder</config-property-value>
</config-property>
<!--The property 'password' has been removed.  'AdminSecret' is used in
This is due to the fact that we have added algorithm name padding in th
the algorithm name (for ex, PBES) with its own handlers.  This crashes
```

2. Geben Sie in der Eigenschaft "UserName" das Konto an, das verwendet wird, um mit CA SiteMinder zu kommunizieren. Verwenden Sie zum Beispiel das SiteMinder-Konto (Standardwert).

## Falscher geheimer Admin-Schlüssel

**Symptom:**

Falscher geheimer Admin-Schlüssel

**Lösung:**

Wird ein falscher geheimer Admin-Schlüssel angegeben, wird in "ra.xml" der Fehler über ungültige Anmeldeinformationen "Cannot connect to policy server: Invalid credentials" wie in der folgenden Abbildung dargestellt angezeigt:

```
2010-12-13 10:35:52,965 WARN  [ims.default] ################################################
2010-12-13 10:35:52,965 WARN  [ims.default] ---- CA IAM FW Startup Sequence Initiated. ----
2010-12-13 10:35:52,965 WARN  [ims.default] * Startup Step 1 : Attempting to start ServiceLocator.
2010-12-13 10:35:53,137 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Task Persistence is up to date.
2010-12-13 10:35:53,153 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Archive is up to date.
2010-12-13 10:35:53,184 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Auditing is up to date.
2010-12-13 10:35:53,231 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Report Snapshot is up to date.
2010-12-13 10:35:53,231 WARN  [ims.default] * Startup Step 2 : Attempting to start PolicyServerService
2010-12-13 10:35:54,934 ERROR [com.netegrity.crypto.PBESHA1RC2CBCPKCS12PBE5128Handler]
com.rsa.jsafe.JSAFE_InputException: Unexpected padding chars
2010-12-13 10:35:54,965 WARN  [org.jboss.resource.connectionmanager.JBossManagedConnectionPool] Throwable while
attempting to get a new connection: null
javax.resource.spi.EISSystemException: Cannot connect to policy server: Invalid credentials
      at com.netegrity.ra.policyserver.impl.PSManagedConnectionFactory.createManagedConnection
```

**Gehen Sie wie folgt vor:**

1. Überprüfen Sie die Eigenschaft "AdminSecret" in "ra.xml".

```
-->
<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
```

2. Geben Sie in der Eigenschaft "AdminSecret" das verschlüsselte Kennwort für den in der UserName-Eigenschaft verwendeten Benutzernamen an.

**Weitere Informationen:**

Ändern eines SiteMinder-Kennworts oder gemeinsamen geheimen Schlüssels (siehe Seite 371)

## Falscher Agentenname

**Symptom:**

Falscher Agentenname

**Lösung:**

Wird ein falscher Agentenname angegeben, wird in "ra.xml" der Initialisierungsfehler "Cannot connect to policy server: Failed to init Agent API: -1" wie in der folgenden Abbildung dargestellt angezeigt:

```
2010-12-13 10:40:08,747 WARN  [ims.default] # IAM Framework 12.5.4.0.461
2010-12-13 10:40:08,747 WARN  [ims.default] ################################################
2010-12-13 10:40:08,747 WARN  [ims.default] ################################################
2010-12-13 10:40:08,747 WARN  [ims.default] # CA Identity Manager 12.5.4.0.461
2010-12-13 10:40:08,747 WARN  [ims.default] ################################################
2010-12-13 10:40:08,747 WARN  [ims.default] ---- CA IAM FW Startup Sequence Initiated. ----
2010-12-13 10:40:08,747 WARN  [ims.default] * Startup Step 1 : Attempting to start ServiceLocator.
2010-12-13 10:40:08,903 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Task Persistence is up to date.
2010-12-13 10:40:08,934 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Archive is up to date.
2010-12-13 10:40:08,981 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Auditing is up to date.
2010-12-13 10:40:09,028 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Report Snapshot is up to date.
2010-12-13 10:40:09,028 WARN  [ims.default] * Startup Step 2 : Attempting to start PolicyServerService
2010-12-13 10:40:10,543 WARN  [org.jboss.resource.connectionmanager.JBossManagedConnectionPool] Throwable while
attempting to get a new connection: null
javax.resource.spi.EISSystemException: Cannot connect to policy server: Failed to init Agent API: -1
      at com.netegrity.ra.policyserver.impl.PSManagedConnectionFactory.createManagedConnection
(PSManagedConnectionFactory.java:299)
      at org.jboss.resource.connectionmanager.InternalManagedConnectionPool.createConnectionEventListener
```

**Gehen Sie wie folgt vor:**

1. Überprüfen Sie die Eigenschaft "AgentName" in "ra.xml".

   ```
   </config-property>
   <config-property>
       <config-property-name>AgentName</config-property-name>
       <config-property-type>java.lang.String</config-property-type>
       <config-property-value>idmagent</config-property-value>
   </config-property>
   <config-property>
   ```

2. Geben Sie den 4.X-Agentennamen an, den Sie während Schritt 3 der SiteMinder-Konfiguration erstellt haben.

## Falscher geheimer Agentenschlüssel

**Symptom:**

Falscher geheimer Agentenschlüssel

**Lösung:**

Wird ein falscher geheimer Agentenschlüssel angegeben, wird in "ra.xml" der Initialisierungsfehler "Cannot connect to policy server: Failed to init Agent API: -1" mit einem vorangestellten Fehler des Verschlüsselungshandlers wie in der folgenden Abbildung dargestellt angezeigt:

```
2010-12-13 10:42:54,622 WARN  [ims.default] Copyright 2000 - 2010 CA. All Rights Reserved
2010-12-13 10:42:54,653 WARN  [ims.default] ################################################
2010-12-13 10:42:54,653 WARN  [ims.default] # IAM Framework 12.5.4.0.461
2010-12-13 10:42:54,653 WARN  [ims.default] ################################################
2010-12-13 10:42:54,653 WARN  [ims.default] ################################################
2010-12-13 10:42:54,653 WARN  [ims.default] # CA Identity Manager 12.5.4.0.461
2010-12-13 10:42:54,653 WARN  [ims.default] ################################################
2010-12-13 10:42:54,653 WARN  [ims.default] ---- CA IAM FW Startup Sequence Initiated. ----
2010-12-13 10:42:54,653 WARN  [ims.default] * Startup Step 1 : Attempting to start ServiceLocator.
2010-12-13 10:42:54,809 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Task Persistence is up to date.
2010-12-13 10:42:54,840 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Archive is up to date.
2010-12-13 10:42:54,887 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Auditing is up to date.
2010-12-13 10:42:54,918 WARN  [ims.tmt.CreateDatabaseSchema] ****** Schema for: Report Snapshot is up to date.
2010-12-13 10:42:54,918 WARN  [ims.default] * Startup Step 2 : Attempting to start PolicyServerService
2010-12-13 10:42:54,934 ERROR [com.netegrity.crypto.PBESHA1RC2CBCPKCS12PBE5128Handler]
com.rsa.jsafe.JSAFE_InputException: Unexpected padding chars
2010-12-13 10:43:04,262 WARN  [org.jboss.resource.connectionmanager.JBossManagedConnectionPool] Throwable while
attempting to get a new connection: null
javax.resource.spi.EISSystemException: Cannot connect to policy server: Failed to init Agent API: -1
      at com.netegrity.ra.policyserver.impl.PSManagedConnectionFactory.createManagedConnection
(PSManagedConnectionFactory.java:299)
```

**Gehen Sie wie folgt vor:**

1. Überprüfen Sie die Eigenschaft "AgentSecret" in "ra.xml".

```
<config-property>
    <config-property-name>AgentSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
```

2. Geben Sie das verschlüsselte Kennwort an, das verwendet wurde, als Sie diesen Agenten erstellt haben.

**Weitere Informationen:**

Ändern eines SiteMinder-Kennworts oder gemeinsamen geheimen Schlüssels (siehe Seite 371)

## Kein Benutzerkontext in CA IdentityMinder

**Symptom:**

Kein Benutzerkontext in CA IdentityMinder

Wenn ein Benutzer versucht, auf CA IdentityMinder ohne einen SMSESSION-Cookie zuzugreifen, kann CA IdentityMinder den Benutzer nicht authentifizieren. In diesem Fall können Sie eine leere CA IdentityMinder-Benutzeroberfläche erwarten.

Wenn Sie den Workflow für Ihre Umgebung aktiviert haben, sehen Sie etwa folgenden Fehler.

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

**Lösung:**

Ein paar Dinge können dies verursachen, aber es ist üblicherweise eines des Folgenden:

- Sie haben direkt auf CA IdentityMinder zugegriffen.
- Der SiteMinder-Agent am Proxy ist deaktiviert (das heißt, nichts ist geschützt – der SMSESSION-Cookie wird nicht erstellt).
- Die SiteMinder-Domäne für die CA IdentityMinder-Umgebung ist falsch konfiguriert.

Die ersten beiden Ursachen sind ziemlich offensichtlich. Vergewissern Sie sich, dass Sie über den Webserver mit dem voll funktionsfähigen, aktivierten Web-Agenten umleiten. Wenn Sie allerdings über den Webserver gehen und der Agent aktiviert ist, müssen Sie die Domäne ändern.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich auf der SiteMinder-Verwaltungsoberfläche an.
2. Finden Sie Ihre CA IdentityMinder-Domäne, und klicken Sie durch die Schichten, um sie zu ändern. Klicken Sie auf die Registerkarte "Bereich" und dann auf den ersten Bereich in der Liste.
3. Der Standardspeicherort des Schrägstrichs ist unter dem Bereich. Löschen Sie ihn.
4. Klicken Sie in die Regel unter diesem Bereich.

   Die standardmäßige Ressource für die Regel ist ein Sternchen "*".
5. Fügen Sie den Schrägstrich "/" vor dem Sternchen hinzu.

   Sie haben den Schrägstrich vom Bereich zur Regel verschoben. Der Schutz ist der gleiche, aber SiteMinder behandelt es anders.

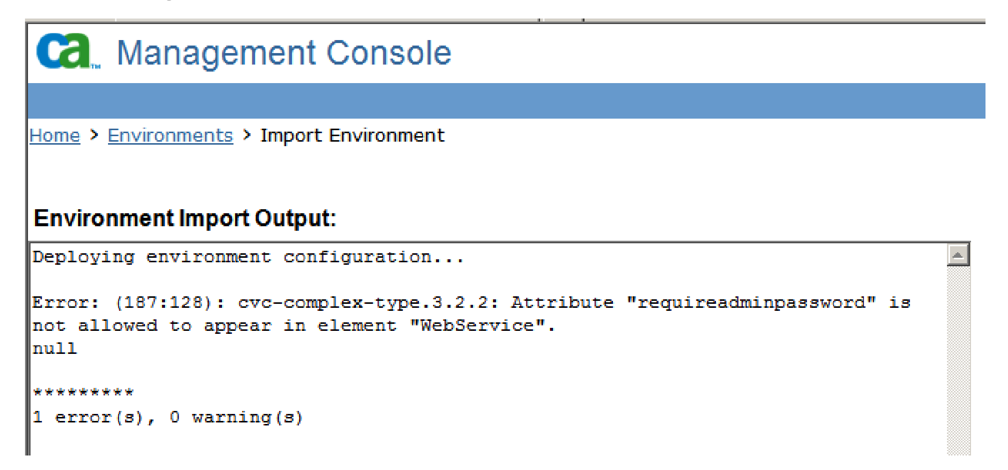
   Sie können sich erfolgreich bei CA IdentityMinder durch SiteMinder anmelden. Um den ordnungsgemäßen Schutz zu validieren, überprüfen Sie Ihre SiteMinder-Agentenprotokolle.

## Fehler beim Laden der Umgebungen

Symptom:

Wenn man eine Umgebung nach der Integration mit SiteMinder zurück in CA IdentityMinder importiert, wird ein Fehler bezüglich des Attributs "requireadminpassword" und des Elements "WebService" angezeigt.

**Hinweis:** Dieses Problem kann auch auftreten, wenn SiteMinder nicht Teil der Bereitstellung ist.




Lösung:

Dieser Fehler erlaubt eine teilweise Bereitstellung der Umgebung. Die teilweise Bereitstellung kann leere Elemente im CA IdentityMinder-Objektspeicher erstellen. Korrigieren Sie eine der Umgebungs-XMLs, und importieren Sie erneut.

**Gehen Sie wie folgt vor:**

1. Suchen Sie die archivierte ZIP-Datei, und überprüfen Sie sie.
2. Erstellen Sie eine Kopie von "XXX_environment_settings.xml".
3. Bearbeiten Sie diese Datei, und suchen Sie das "WebService"-Element.
4. Löschen Sie den Tag "requireadminpassword="false".

   Hinweis: Entfernen Sie den Tag *und* den Wert. Entfernen Sie nicht nur den Wert.
5. Speichern Sie Ihre Änderungen, und fügen Sie die Datei zurück in die ZIP-Datei ein.
6. Importieren Sie die archivierte Umgebungs-ZIP-Datei erneut.

   Sie müssen die Umgebung nicht löschen, die aus dem fehlgeschlagenen Versuch erstellt wurde. Beim erneuten Importieren behebt eine korrigierte Datei die Fehler des fehlgeschlagenen Versuchs.

## CA IdentityMinder-Verzeichnis oder -Umgebung kann nicht erstellt werden

**Symptom:**

Es kann kein CA IdentityMinder-Verzeichnis oder -Umgebung erstellt werden, wenn SiteMinder-Integration aktiviert ist.

**Lösung:**

Dieses Problem kann von einer fehlenden Eingabe in der Registrierung verursacht werden.

Überprüfen Sie, dass die folgende Registrierungseinstellung auf dem SiteMinder-Richtlinienserver-Rechner vorhanden ist:

- Solaris oder Linux:

  Überprüfen Sie, dass die folgende Eingabe in "sm.registry" vorhanden ist: ImsInstalled=8.0; REG_SZ

- Windows:

  Überprüfen Sie, dass "ImsInstalled=8.0; REG_SZ" am folgenden Speicherort vorhanden ist:
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  **Hinweis**: Wenn der Registrierungspfad "\Netegrity\SiteMinder\CurrentVersion" nicht vorhanden ist, erstellen Sie ihn manuell.

Wenn Sie die Registrierung ändern, müssen Sie den Richtlinienserver neu starten, damit die Änderungen in Kraft treten.

**Wichtig!** Bevor Sie die Registrierung ändern, führen Sie eine vollständige Systemsicherung aus.

## Benutzer kann sich nicht anmelden

**Symptom:**

Ein neuer Benutzer kann sich nicht in einer Umgebung mit einem Klartextkennwort anmelden.

**Lösung:**

Überprüfen Sie, dass die folgende Datenklassifizierung nicht in die Kennwortattributdefinition in der Verzeichniskonfigurationsdatei (directory.xml) eingeschlossen ist:

<DataClassification name="AttributeLevelEncrypt"/>

In Umgebungen, die die folgenden Komponenten einschließen, werden bei Verschlüsselung der Kennwörter auf Attributebene Benutzer daran gehindert, sich anzumelden:

- CA SiteMinder und
- Eine relationale Datenbank

# So konfigurieren Sie CA IdentityMinder-Agent-Einstellungen

Wenn CA IdentityMinder in SiteMinder integriert wird, verwendet CA IdentityMinder einen integrierten CA IdentityMinder-Agenten, um mit dem SiteMinder-Richtlinienserver zu kommunizieren. Um die Leistung zu optimieren, konfigurieren Sie die folgenden Verbindungseinstellungen für den CA IdentityMinder-Agenten.

1. Führen Sie einen der folgenden Schritte durch:
   - Wenn CA IdentityMinder auf einem WebLogic- oder WebSphere-Anwendungsserver ausgeführt wird, bearbeiten Sie den Ressourcenadapter im Connector-Deskriptor "policyserver_rar" in der Konsole des Anwendungsservers.
   - Wenn CA IdentityMinder auf einem JBoss-Anwendungsserver ausgeführt wird, öffnen Sie "policyserver-service.xml" in "<JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF".
2. Konfigurieren Sie die Einstellungen wie folgt:

   **ConnectionMax**

   Legt die Höchstanzahl von Verbindungen zum Richtlinienserver fest, zum Beispiel 20.

**ConnectionMin**

Legt die Mindestanzahl von Verbindungen zum Richtlinienserver fest, zum Beispiel 2.

**ConnectionStep**

Legt die Anzahl von zusätzlichen Verbindungen fest, die geöffnet werden, wenn alle Agent-Verbindungen verwendet werden.

**ConnectionTimeout**

Gibt den Zeitbetrag in Sekunden an, die der Agent auf die Verbindung mit SiteMinder warten muss, bevor eine Zeitüberschreitung eintritt.

3. Starten Sie den Anwendungsserver neu.

# Konfigurieren der SiteMinder-Hochverfügbarkeit

Wenn Sie einen SiteMinder-Richtlinienserver-Cluster erstellt haben, können Sie einen Anwendungsserver-Cluster konfigurieren, um ihn für Lastenausgleich und Failover zu verwenden.

**Gehen Sie wie folgt vor:**

1. Bearbeiten Sie die Datei "ra.xml" an diesem Speicherort:
   `WebSphere:`
   *`WAS_PROFILE`*`/config/cells/`*`CELL_NAME`*`/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF`
   `Jboss:`*`jboss_home`*`/server/all/deploy/iam_im.ear/policyserver_rar/META-INF`
   `WebLogic: `*`wl_domain`*`/applications/iam_im.ear/policyserver_rar/META-INF`
2. Ändern Sie diese Elemente, die in den nachfolgenden Abschnitten erklärt werden:
   - Verbindungseinstellungen für den Richtlinienserver
   - Die Anzahl von Richtlinienservern
   - Die Auswahl von Lastenausgleich oder Failover für den Cluster.
3. Wiederholen Sie diese Schritte für jeden CA IdentityMinder-Server im Cluster.
4. Starten Sie den Anwendungsserver neu, damit die Änderungen wirksam werden.

**Hinweis**: Wenn Sie ein CA IdentityMinder-Verzeichnis oder eine Umgebung erstellen oder Verzeichnis- oder Umgebungseinstellungen ändern, legen Sie SiteMinder-Failover und FailoverServers auf "false" fest. Andernfalls könnte das Verzeichnisobjekt zwar erstellt, aber nicht rechtzeitig zur Verwendung repliziert werden. Beispielsweise erstellen Sie ein Verzeichnis auf Server 1. Dann erstellen Sie ein Attribut unter Verwendung der Objekt-ID von diesem Verzeichnis auf Server 2, aber das zweite Verzeichnis ist noch nicht vorhanden. Es wird ein Fehler über nicht gefundene Objekte angezeigt.

## Ändern der Richtlinienserver-Verbindungseinstellungen

Die Richtlinienserver-Verbindungsinformationen müssen den Primärserver für die Produktionsumgebung widerspiegeln. Diese Information besteht aus ConnectionURL, dem Benutzernamen und Kennwort für das SiteMinder-Admin-Konto, und dem Namen sowie dem gemeinsamen geheimen Schlüssel für den Agenten.

Im folgenden Beispiel werden die bearbeitbaren Werte in GROSSBUCHSTABEN angezeigt.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</co
nfig-
                property-value>
</config-property>

<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

**Hinweis**: Verwenden Sie für die Werte, die verschlüsselten Text erfordern, das CA IdentityMinder-Kennwort-Tool. Weitere Informationen finden Sie im *Konfigurationshandbuch*.

## Hinzufügen von mehreren Richtlinienservern

Um mehr Richtlinienserver zur CA IdentityMinder-Installationsinstanz hinzuzufügen, bearbeiten Sie den Eintrag "FailoverServers" in der Datei "ra.xml".

**Hinweis**: Schließen Sie den primären Richtlinienserver und alle Failover-Server in den Eintrag "FailoverServers" ein.

Geben Sie für jeden Richtlinienserver eine IP-Adresse und Portnummern für Authentifizierung, Autorisierung und Kontodienste ein. Verwenden Sie ein Semikolon, um Eingaben voneinander zu trennen, wie hier angezeigt:

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

## Auswählen von Lastenausgleich oder Failover

Das Standardverhalten von CA IdentityMinder ist die Verwendung von Round-Robin-Lastenausgleich mithilfe der Server, die durch "ConnectionURL" und "FailoverServers" identifiziert werden. Lastenausgleich tritt auf, wenn Sie "FailOver" auf "false" lassen.

Um das Failover auszuwählen, setzen Sie "FailOver" auf "true":

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

# Entfernen von SiteMinder aus einer vorhandenen CA IdentityMinder-Bereitstellung

Dieser Abschnitt enthält detaillierte Anweisungen für das Entfernen von CA SiteMinder aus einer vorhandenen CA IdentityMinder-Umgebung.

**Gehen Sie wie folgt vor:**

**Wichtig!** Kennwortverlaufsinformationen sind nach der Migration nicht mehr abrufbar.

1. Halten Sie den Anwendungsserver an.
2. Deaktivieren Sie den Richtlinienserver in der Datei "ra.xml", die sich in "\iam_im.ear\policyserver.rar\META-INF" befindet, indem Sie den Wert für "config-property" "Enabled" auf "false" festlegen.
3. Bearbeiten Sie die Datei "web.xml" unter "\iam_im.ear\User_console.war/WEB-INF", und legen Sie die Eigenschaft "FrameworkAuthFilter" auf "Enabled = true" fest.

   **Hinweis:** Für WebSphere befindet sich die Datei "web.xml" unter "*WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF".
4. Starten Sie den Anwendungsserver.
5. (Nur WebSphere) Aktualisieren Sie das policyServer-Objekt in der Verwaltungskonsole mit den gleichen Werten wie in der Datei "ra.xml".

# SiteMinder-Vorgänge

In den folgenden Abschnitte wird erläutert, wie Sie SiteMinder-Funktionen, einschließlich Richtliniendomänen und Authentifizierungsschemen ändern, um CA IdentityMinder zu unterstützen:

**Erfassen von Benutzeranmeldeinformationen mithilfe eines benutzerdefinierten Authentifizierungsschemas** **(siehe Seite 351)**

Ändert die Methode, die CA IdentityMinder verwendet, um Anmeldeinformationen für Benutzer zu erfassen, die versuchen, auf eine CA IdentityMinder-Umgebung zuzugreifen.

**Konfigurieren von Zugriffsrollen** **(siehe Seite 353)**

Legt den Zugriff auf Funktionen in einer Anwendung fest.

**Konfigurieren der LogOff-URL** **(siehe Seite 368)**

Verhindert unbefugten Zugriff auf eine CA IdentityMinder-Umgebung durch das Erzwingen einer vollständigen Abmeldung.

**Aktualisieren eines Alias in SiteMinder-Bereichen (siehe Seite 370)**

Aktualisiert die Bereiche, die eine CA IdentityMinder-Umgebung schützen, wenn Sie den Aliasnamen der Umgebung ändern.

**SiteMinder-Kennwörter (siehe Seite 371)**

Lässt Sie das Kennwort für das Administratorkonto, das CA IdentityMinder verwendet, um mit SiteMinder zu kommunizieren, und den gemeinsamen geheimen Schlüssel für den SiteMinder-Agenten ändern, der eine CA IdentityMinder-Umgebung schützt.

**Konfigurieren der CA IdentityMinder-Agent-Einstellungen (siehe Seite 346)**

Optimiert die Leistung des CA IdentityMinder-Agenten, der mit dem SiteMinder-Richtlinienserver kommuniziert.

**Verwenden von unterschiedlichen Verzeichnissen für Authentifizierung und Autorisierung (siehe Seite 373)**

Befähigt Administratoren, die Profile in einem Verzeichnis haben, Benutzer in einem anderen Verzeichnis zu verwalten.

**Verbessern der Leistung von LDAP-Verzeichnisvorgängen (siehe Seite 375)**

Erhöht den Durchsatz von CA IdentityMinder-Anfragen an den Benutzerspeicher, indem man SiteMinder konfiguriert, um mehrere Verbindungen für das gleiche Verzeichnis zu öffnen.

## Erfassen von Benutzeranmeldeinformationen mithilfe eines benutzerdefinierten Authentifizierungsschemas

SiteMinder verwendet ein Authentifizierungsschema, um Benutzeranmeldeinformationen zu erfassen und die Identität eines Benutzers bei der Anmeldung zu bestimmen. Sobald ein Benutzer identifiziert ist, generiert CA IdentityMinder eine persönliche Benutzerkonsole, die auf den Berechtigungen des Benutzers basiert.

Sie können ein SiteMinder-Authentifizierungsschema implementieren, um eine CA IdentityMinder-Umgebung zu schützen.

Zum Beispiel können Sie ein Authentifizierungsschema für HTML-Formulare implementieren, das Anmeldeinformationen in einem HTML-Formular erfasst. Das HTML-Formulars lässt Sie eine Anmeldungsseite erstellen, die Markenelemente wie z. B. ein Unternehmenslogo einschließen kann und auf die Seiten für Selbstregistrierung und vergessenene Kennwörter verlinkt ist.

**Hinweis:** Weitere Informationen zu Authentifizierungsschemen finden Sie im *Konfigurationshandbuch für CA SiteMinder-Richtlinienserver*.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei einer der folgenden Schnittstellen an:
   - Für CA SiteMinder Web Access Manager r12 oder höher melden Sie sich bei der Verwaltungsoberfläche an.
   - Für CA eTrust SiteMinder 6.0 SP5 melden Sie sich bei der Richtlinienserver-Benutzeroberfläche an.

   **Hinweis:** Weitere Informationen zur Verwendung dieser Schnittstellen finden Sie in der Dokumentation der SiteMinder-Version, die Sie verwenden.
2. Erstellen Sie ein Authentifizierungsschema, wie im *Konfigurationshandbuch für CA SiteMinder-Richtlinienserver* beschrieben.
3. Ändern Sie den Bereich, der die entsprechende CA IdentityMinder-Umgebung schützt, um das Authentifizierungsschema zu verwenden, das Sie in Schritt 1 erstellt haben.

   Der Bereichsname hat das folgende Format:

   *Identity Manager-Umgebung*_ims_realm

   **Hinweis:** Wenn Sie Support für öffentliche Aufgaben konfiguriert haben, sehen Sie einen zusätzlichen Bereich, *Identity Manager-Umgebung*_pub_realm. Dieser Bereich verwendet ein anonymes Authentifizierungsschema, um unbekannten Benutzern zu ermöglichen, die Funktionen für Selbstregistrierung und vergessene Kennwörter zu verwenden, ohne Anmeldeinformationen anzugeben. Ändern Sie die Authentifizierungsschemen für diese Bereiche nicht.

## Importieren von Datendefinitionen in den Richtlinienspeicher

Sie können den Zugriff eines Benutzers auf Anwendungsfunktionen mithilfe von SiteMinder-Richtlinien steuern. Die Richtlinienserver-Installation schließt die erforderlichen Datendefinitionen ein, um diese Steuerung zu ermöglichen. Importieren Sie die Datei "IdmSmObjects.xdd" von diesem Speicherort:

*siteminder_home*\xps\dd

*siteminder_home* ist der Richtlinienserver-Installationspfad.

## Planen von Zugriffsrollen

Um den Zugriff auf Anwendungen zu steuern, erstellen Sie Zugriffsrollen und Aufgaben. Eine Zugriffsaufgabe gibt den Zugriff auf eine Funktion in einer Anwendung an. Eine Zugriffsrolle enthält eine oder mehrere Zugriffsaufgaben für eine oder mehrere Anwendungen. Wenn eine Zugriffsrolle einem Benutzer zugewiesen worden ist, kann der Benutzer die Funktionen verwenden, die in dieser Rolle vorhanden sind.

Zugriffsrollen für Anwendungszugriff enthält weitere Details zum Zweck von Zugriffsrollen.

Zugriffsrollen erfordern die Konfiguration in Identity Manager und SiteMinder. Zwei Administratoren müssen beteiligt werden:

- Identity Manager-Administrator – Muss fähig sein, Zugriffsrollen und Aufgaben in Identity Manager zu erstellen. Die Standardrollen "System-Manager" und "Zugriffsrollen-Manager" schließen diese Aufgaben ein.
- SiteMinder-Administrator – Muss einen Systemgeltungsbereich haben und System- und Domänenobjekte verwalten können. Weitere Informationen dazu finden Sie unter *CA eTrust SiteMinder-Richtliniendesign*.

**Hinweis:** Die Richtliniendesign-Benutzeroberfläche verwendet den Begriff *Identity Manager-Umgebung,* um sich auf das zu beziehen, was jetzt eine *Identity Manager-Umgebung* genannt wird. Die mit diesem Produkt gelieferte SiteMinder-Dokumentation bezeichnet dies auch als *Identity Manager*. Ab r8.1 ist der neue Produktname *Identity Manager*.

Der folgende Vorgang umfasst die Schritte zum Erstellen einer Zugriffsrolle:

1. Ein Identity Manager-Administrator mit der Rolle für Zugriffsrollen-Manager:
    a. Erstellt Zugriffsaufgaben.
    b. Erstellt eine Zugriffsrolle.
    c. Teilt dem SiteMinder-Administrator Rollen- und Aufgabeninformationen mit.

2. Ein SiteMinder-Administrator erstellt ein rollenbasierte Zugriffssteuerungsrichtlinie wie folgt:

    a. Zuordnen eines Benutzerverzeichnisses, das mit einer oder mehreren Identity Manager-Umgebungen verknüpft ist, zu einer Richtliniendomäne.

    b. Zuordnen von einer oder mehreren Identity Manager-Umgebungen zur Richtliniendomäne in Schritt 1.

    c. Erstellen von Bereichen und Regeln in der Richtliniendomäne (wenn sie nicht bereits vorhanden sind). Die Bereiche und Regeln sollten den Ressourcen entsprechen, auf welche die Zugriffsrollen Zugriff erteilen werden.

    d. Erstellen von Richtlinien und Zuordnen zu Rollen in der Identity Manager-Umgebung.

    e. (Optional) Angabe von Antworten, die den geschützten Ressourcen Berechtigungsinformationen liefern.

    Anweisungen zu den vorangehenden Schritten finden Sie unter *CA eTrust SiteMinder-Richtliniendesign*.

## Aktivieren von Zugriffsrollen zur Verwendung mit SiteMinder

Um Zugriffsrollen mit CA SiteMinder zu verwenden, spiegelt CA IdentityMinder alle Objekte im CA IdentityMinder-Objektspeicher, die sich auf diese Zugriffsrollen beziehen, im SiteMinder-Richtlinienspeicher. Um dies zu ermöglichen, konfigurieren Sie eine Eigenschaft in der CA IdentityMinder-Management-Konsole.

**So aktivieren Sie Zugriffsrollen für die Verwendung mit SiteMinder**

1. Öffnen Sie die Managementkonsole.

2. Wählen Sie "Umgebung", "*Ihre Umgebung*", "Erweiterte Einstellungen", "Verschiedenes".

3. Fügen Sie eine neue Eigenschaft durch das Angeben der folgenden Informationen hinzu:

    ■ Geben Sie im Feld "Eigenschaft" Folgendes ein:

      EnableSMRBAC

    ■ Geben Sie im Feld "Wert" Folgendes ein:

      true

4. Klicken Sie auf "Hinzufügen". Klicken Sie dann auf "Speichern".

   Eine Meldung, die anzeigt, dass die Umgebung neu gestartet werden muss, wird angezeigt.

5. Starten Sie die Umgebung neu.

   CA IdentityMinder unterstützt jetzt Zugriffsrollen und Aufgaben für die Verwendung mit CA SiteMinder.

Sobald Sie Zugriffsrollen für die Verwendung mit CA SiteMinder aktivieren, beachten Sie Folgendes:

- Wenn Sie Zugriffsrollen in CA Identity Manager r8x verwendet haben, müssen Sie einen zusätzlichen Migrationsschritt ausführen, um diese Zugriffsrollen in der aktuellen Version von CA IdentityMinder zu verwalten. Weitere Informationen finden Sie im *Aktualisierungshandbuch*.
- Um die Unterstützung von Zugriffsrollen in SiteMinder zu deaktivieren, löschen Sie die CA IdentityMinder-Zugriffsrolle und Aufgabenobjekte aus dem SiteMinder-Richtlinienspeicher. Entfernen Sie dann die Eigenschaft "EnableSMRBAC" aus der Liste mit verschiedenen Eigenschaften, und starten Sie die Umgebung neu.

## Hinzufügen einer Zugriffsaufgabe zur Admin-Rolle

Standardmäßig werden die Zugriffsaufgaben nicht auf der Registerkarte "Rollen und Aufgaben" angezeigt, Sie müssen die Zugriffsaufgaben zur Admin-Rolle des angemeldeten Benutzers hinzufügen.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei einem CA IdentityMinder-Konto mit einer Rolle an, die eine Aufgabe für das Erstellen von Zugriffsrollen einschließt.
2. Klicken Sie auf "Rollen und Aufgaben", "Admin-Rolle ändern".
3. Wählen Sie die Admin-Rolle des angemeldeten Benutzers aus.
4. Klicken Sie auf die Registerkarte "Aufgaben", Feld "Nach Kategorie filtern", und wählen Sie "Rollen und Aufgaben" aus der Dropdown-Liste aus.
5. Wählen Sie in der Dropdown-Liste "Aufgabe hinzufügen" die Option "Zugriffsaufgabe erstellen" aus.
6. Klicken Sie auf "Senden".

## Erstellen von Zugriffsaufgaben

Eine Zugriffsaufgabe ist eine einzelne Aktion, die ein Benutzer in einer Unternehmensanwendung ausführen kann, wie beispielsweise eine Bestellung in einer Finanzanwendung zu generieren. Benutzer können diese Aktion ausführen, wenn ihnen eine Zugriffsrolle zugewiesen wird, die die Zugriffsaufgabe einschließt.

**Wichtig!** Um eine Zugriffsaufgabe zu erstellen, müssen Sie die Zugriffsaufgaben (siehe Seite 355) zur Admin-Rolle des angemeldeten Benutzers hinzufügen.

**Gehen Sie wie folgt vor:**

1. Wählen Sie "Rollen und Aufgaben", "Zugriffsaufgaben", "Zugriffsaufgabe erstellen" aus.
2. Wählen Sie eine der folgenden Optionen aus:
   - Zugriffsaufgabe erstellen
   - Kopie einer Zugriffsaufgabe erstellen
3. Füllen Sie diese Felder aus:

   **Name**

   Ein eindeutiger Name, den Sie der Aufgabe zuweisen können, wie "Auftrag generieren".

   **Tag**

   Eindeutiger Tag für die Aufgabe. Der Tag muss mit einem Buchstaben oder Unterstrich beginnen und darf nur Buchstaben, Ziffern oder Unterstriche enthalten.

   **Beschreibung**

   Ein optionaler Hinweis auf den Zweck der Aufgabe.

   **Anwendungs-ID**

   Ein Bezeichner für eine Anwendung, beispielsweise den Anwendungsnamen, der mit der Aufgabe verknüpft ist. Die Anwendungs-ID kann Leerzeichen oder nicht-alphanumerische Zeichen enthalten.

   Notieren Sie sich diese ID; Sie benötigen sie, wenn Sie die Rolle in SiteMinder aktivieren.
4. Um die Zugriffsaufgabe abzuschließen, klicken Sie auf "Senden".

## So erstellen Sie eine Zugriffsrolle

Eine Zugriffsrolle enthält Zugriffsaufgaben, die den Zugriff auf Funktionen in einer Anwendung festlegen. Zum Beispiel kann eine Rolle Aufgaben enthalten, die Rollenmitgliedern ermöglichen, eine Bestellung in eine Einkaufsanwendung einzugeben und Mengen in einer Inventarerfassungsanwendung zu aktualisieren.

Führen Sie folgende Schritte aus, um eine Zugriffsrolle zu erstellen:

1. Beginnen Sie mit der Erstellung einer Zugriffsrolle. (siehe Seite 357)
2. Definieren Sie grundlegende Eigenschaften für die Zugriffsrolle in der Registerkarte "Profil". (siehe Seite 357)
3. Wählen Sie Zugriffsaufgaben für die Rolle aus. (siehe Seite 358)
4. Definieren Sie Mitgliederrichtlinien für die Rolle. (siehe Seite 359)
5. Definieren Sie Admin-Richtlinien für die Rolle. (siehe Seite 360)
6. Definieren Sie Eigentümerregeln für die Rolle. (siehe Seite 361)

## Beginnen Sie mit der Erstellung einer Zugriffsrolle

1. Melden Sie sich bei einem Identity Manager-Konto mit einer Rolle an, die eine Aufgabe zum Erstellen von Zugriffsrollen enthält.
2. Klicken Sie auf die Option "Zugriffsrollen" und dann auf die Option "Zugriffsrolle erstellen".

   Wählen Sie die Option aus, um eine neue Rolle oder eine Kopie einer Rolle zu erstellen. Wenn Sie die Option "Kopieren" auswählen, suchen Sie die Rolle.
3. Fahren Sie mit dem nächsten Abschnitt fort,Definieren des Profils für Zugriffsrollen.

## Definieren des Profils für Zugriffsrollen

**So definieren Sie das Profil für Zugriffsrollen:**

1. Geben Sie einen Namen und eine Beschreibung ein, und vervollständigen Sie alle benutzerdefinierten Attribute, die für die Rolle definiert sind.

   **Hinweis:** Sie können auf dem Register "Profil" benutzerdefinierte Attribute angeben, die weitere Informationen zu Zugriffsrollen enthalten. Sie können diese zusätzlichen Informationen verwenden, um Rollensuchvorgänge in Umgebungen zu erleichtern, die eine große Anzahl von Rollen enthalten.
2. Wählen Sie die Option "Aktiviert" aus, wenn Sie die Rolle sofort nach der Erstellung für die Verwendung freigeben möchten.
3. Fahren Sie mit dem nächsten Abschnitt, Definieren von Mitgliederrichtlinien für Zugriffsrollen, fort.

## Auswählen von Zugriffsaufgaben für die Rolle

Gehen Sie auf der Registerkarte "Aufgaben" wie folgt vor:

1. Wählen Sie die in diese Rolle einzuschließenden Aufgaben aus. Wählen Sie zuerst die Anwendungen aus, dann die Aufgabe. Sie können Aufgaben aus verschiedenen Anwendungen einbeziehen:

   **Hinweis:** Wenn eine andere Rolle die Aufgaben hat, die Sie benötigen, klicken Sie auf "Aufgaben aus einer anderen Rolle kopieren". Sie können die angezeigte Liste bearbeiten.

   Beim Erstellen einer Rolle oder Aufgabe sehen Sie Symbole zum Hinzufügen, Bearbeiten und Entfernen von Elementen:

   Weitergehen oder das aktuelle Element auswählen, um es anzuzeigen oder zu bearbeiten.

   Wenn JavaScript deaktiviert ist, klicken Sie auf die Schaltfläche "Weiter", um aus einer Dropdown-Liste auszuwählen.

   Zurückgehen oder eine frühere Auswahl rückgängig machen.

   Ein Element einfügen, z. B. eine Aufgabe oder Regel.

   Die aktuelle Aufgabe oder (bei Regeln) den folgenden Ausdruck löschen.

   Aktuelles Element in der Liste nach oben verschieben.

   Aktuelles Element in der Liste nach unten verschieben.

2. Fahren Sie mit dem nächsten Abschnitt, Definieren von Admin-Richtlinien für Zugriffsrollen, fort.

## Definieren von Mitgliederrichtlinien für Zugriffsrollen

Eine Mitgliederrichtlinie definiert eine Mitgliederregel und Bereichsregeln für eine Rolle. Sie können verschiedene Mitgliederrichtlinien für eine Rolle definieren. Für jede Richtlinie haben Benutzer, die der Bedingung in der Mitgliederregel entsprechen, den entsprechenden Bereichsumfang bei der Verwendung der Rolle, der in der Richtlinie definiert ist.

**Gehen Sie wie folgt vor:**

1. Wählen Sie die Registerkarte "Mitglieder" aus.
2. Klicken Sie auf "Hinzufügen", um Mitgliederrichtlinien zu definieren.
3. (Optional) Definieren Sie auf der Seite "Mitgliederrichtlinie" optional eine Mitgliederregel für denjenigen, der diese Rolle verwenden können muss.

   Beim Definieren einer Mitgliederregel wird diese Rolle automatisch Benutzern zugeordnet, die mit den Kriterien in der Mitgliederrichtlinie übereinstimmen.

   **Hinweis:** Definieren Sie Mitgliederrichtlinien, die nur Verzeichnisattribute verwenden, zum Beispiel: title=Manager. Wenn Sie Mitgliederrichtlinien definieren, die auf Objekte verweisen, die nicht im Benutzerverzeichnis gespeichert sind, wie Admin-Rollen, kann SiteMinder den Verweis nicht auflösen.

4. Überprüfen Sie, dass die Mitgliederrichtlinie auf der Registerkarte "Mitglieder" angezeigt wird.

   Um eine Richtlinie zu bearbeiten, klicken Sie links auf das Pfeilsymbol. Um sie zu entfernen, klicken Sie auf das Minuszeichen.

5. Aktivieren Sie auf der Registerkarte "Mitglieder" das Kontrollkästchen "Administratoren können Mitglieder dieser Rolle hinzufügen oder aus ihr entfernen".

   Sobald Sie diese Funktion aktivieren, definieren Sie die Aktion zum Hinzufügen und Aktion zum Entfernen. Diese Aktionen definieren, was geschieht, wenn ein Benutzer als ein Rollenmitglied hinzugefügt oder entfernt wird.

## Definieren von Admin-Richtlinien für Zugriffsrollen

Eine Admin-Richtlinie definiert Admin-Regeln, Bereichsregeln und Administratorrechte für eine Rolle. Sie können verschiedene Admin-Richtlinien für eine Rolle definieren. Jede Richtlinie zeigt an, dass, wenn ein Administrator der Bedingung in der Admin-Regel entspricht, er den Bereichsumfang und die Administratorrechte hat, die für die Richtlinie definiert sind.

Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte "Administratoren" für die Zugriffsrolle aus.
2. Wenn Sie die Option "Administratoren verwalten" verfügbar machen wollen, aktivieren Sie das Kontrollkästchen "Administratoren können Mitglieder dieser Rolle hinzufügen oder aus ihr entfernen".

   Sofern Sie diese Funktion aktiviert haben, definieren Sie die Aktionen dafür, wenn ein Benutzer als ein Administrator der Rolle hinzugefügt oder entfernt wird.
3. Fügen Sie auf der Registerkarte "Administratoren" Admin-Richtlinien hinzu, die Admin- und Bereichsregeln sowie Administratorrechte einschließen. Jede Richtlinie benötigt mindestens eine Berechtigung (Mitglieder verwalten oder Administratoren verwalten).

   Sie können mehrere Admin-Richtlinien mit unterschiedlichen Regeln und unterschiedlichen Berechtigungen für Administratoren, die der Regel entsprechen, hinzufügen.

   **Hinweis:** Definieren Sie Admin-Richtlinien, die nur Verzeichnisattribute verwenden, zum Beispiel: title=Manager. Wenn Sie Mitgliederrichtlinien definieren, die auf Objekte verweisen, die nicht im Benutzerverzeichnis gespeichert sind, wie Admin-Rollen, kann SiteMinder den Verweis nicht auflösen.
4. Um eine Richtlinie zu bearbeiten, klicken Sie links auf das Pfeilsymbol. Um sie zu entfernen, klicken Sie auf das Minuszeichen.
5. Fahren Sie mit dem nächsten Abschnitt, Definieren von Eigentümerregeln für Zugriffsrollen, fort.

## Definieren von Eigentümerregeln für Zugriffsrollen

Eine Eigentümerregel definiert, wer eine Rolle ändern kann. Sie können verschiedene Eigentümerregeln für eine Rolle definieren.

Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte "Eigentümer" für die Zugriffsrolle aus.
2. Definieren Sie Eigentümerregeln, die bestimmen, welche Benutzer die Rolle ändern können.

   **Hinweis:** Definieren Sie Eigentümerregeln, die nur Verzeichnisattribute verwenden, zum Beispiel: title=Manager. Wenn Sie Eigentümerregeln definieren, die auf Objekte verweisen, die nicht im Benutzerverzeichnis gespeichert sind, wie Admin-Rollen, kann SiteMinder den Verweis nicht auflösen.
3. Klicken Sie auf "Senden".

   Eine Meldung wird eingeblendet, um anzuzeigen, dass die Aufgabe gesendet worden ist. Es kann eine vorübergehende Verzögerung auftreten, bevor ein Benutzer die Rolle verwenden kann.

## Aktivieren von Zugriffsrollen in SiteMinder

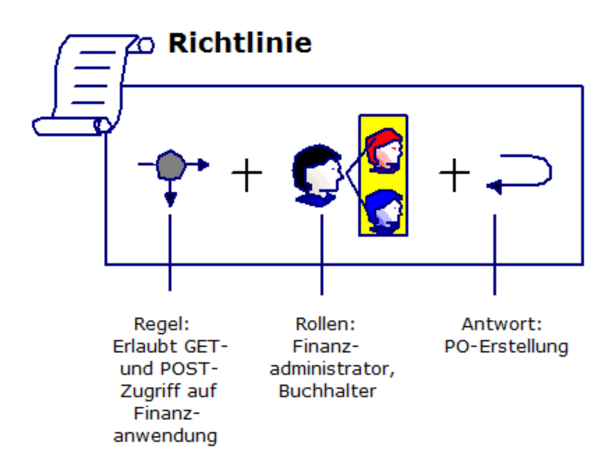
Ein SiteMinder-Administrator bindet Rollen an Sicherheitsrichtlinien, die definieren, wie Benutzer mit Ressourcen interagieren. Richtlinien können die folgenden Objekte verknüpfen:

- Benutzer und Benutzergruppen – Identifizieren ein Set von Benutzern, die von einer Richtlinie betroffen sind.
- Rollen – Identifizieren Benutzer, denen ein Set von Berechtigungen in Identity Manager zugewiesen worden ist.
- Regeln – Identifizieren eine Ressource und die Aktionen, die für die Ressource erlaubt oder unzulässig sind. Die Ressource ist normalerweise eine URL, eine Anwendung oder ein Skript.
- Antworten – Bestimmen eine Reaktion auf eine Regel. Wenn eine Regel ausgelöst wird, werden Antworten an einen SiteMinder-Agenten zurückgegeben.

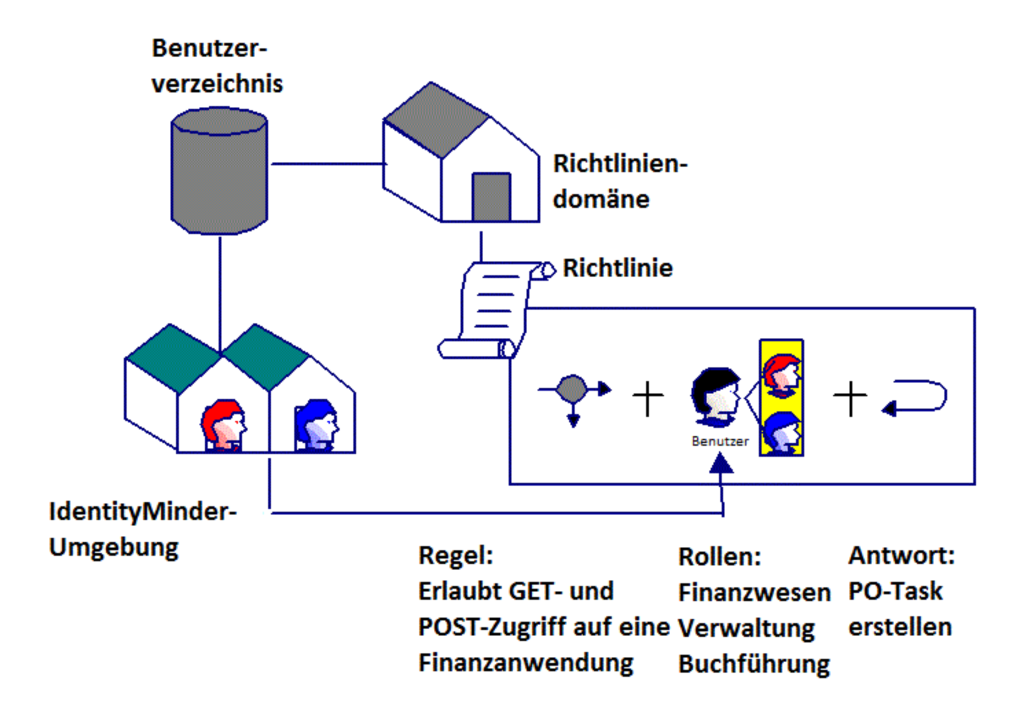
  Identity Manager verwendet SiteMinder-Antworten, um bestimmte Aufgabe und Rolleninformationen zu einer geschützten Ressource zu liefern.

Sie können SiteMinder-Richtlinien an Benutzer, an Rollen oder an Benutzer *und* Rollen binden. Wenn ein Benutzer oder Rollenmitglied versucht, auf eine geschützte Ressource zuzugreifen, verwendet SiteMinder Informationen in der Richtlinie, um zu entscheiden, ob er Zugriff erteilt werden soll, und um Antworten auszulösen.

Die folgende Abbildung veranschaulicht die Beziehung von Richtlinienobjekten in einer rollenbasierten Richtlinie.




SiteMinder-Richtlinien werden in Richtliniendomänen erstellt, die Benutzerverzeichnisse logisch an geschützte Ressourcen binden. Die folgende Abbildung veranschaulicht die Beziehung von Richtlinienobjekten in einer rollenbasierten Richtlinie.



Um einer geschützten Anwendung Benutzerberechtigungen zu liefern, ordnet ein SiteMinder-Administrator eine Regel in der Richtlinie der Anwendung paarweise mit einer Antwort an. Die Antwort enthält ein SiteMinder-generiertes Antwortattribut, das Berechtigungsinformationen aus Identity Manager abruft.

Wenn SiteMinder ein Rollenmitglied für eine geschützte Ressource genehmigt, finden die folgenden Ereignisse statt:

1. Die Regel der Richtlinie wird in SiteMinder ausgeführt und löst die gepaarte Antwort aus.
2. Der Richtlinienserver erhält Berechtigungsinformationen von Identity Manager zum Einschließen in eine Antwort.
3. Der Richtlinienserver übergibt das Antwortattribut an den Web-Agenten.
4. Der Web-Agent macht die Berechtigungsinformationen für die Anwendung als HTTP-Header-Variable oder als Cookie verfügbar.

## SiteMinder-generierte Antwortattribute

Identity Manager übergibt Berechtigungsinformationen durch Antworten von SiteMinder-Web-Agent an Anwendungen. Diese Antworten enthalten HTTP-Header-Variablen in Antwortattributen, die von der Anwendung verwendet werden können, um die Zugriffsberechtigungen eines Benutzers zu bestimmen. Antworten sind in SiteMinder-Richtlinien eingeschlossen, die entscheiden, wie Benutzer mit einer geschützten Ressource interagieren.

SiteMinder-Administratoren können eine Antwort konfigurieren, die zwei Typen von Antwortattributen einschließt, um einer Anwendung Informationen zu übergeben:

- SM_USER_APPLICATION_ROLES[:*Anwendungs-ID*] – Gibt eine Liste von Rollen zurück, die einem Benutzer zugeordnet sind
- SM_USER_APPLICATION_TASKS[:*Anwendungs-ID*] – Gibt eine Liste von Aufgaben zurück, die ein Benutzer basierend auf ihm zugewiesenen Rollen ausführen kann

Die Anwendungs-ID beschränkt das angeforderte Set von Rollen und Aufgaben auf eine bestimmte Anwendung. Wenn Sie beispielsweise das folgende Antwortattribut erstellen:

SM_USER_APPLICATION_ROLES:Finanzanwendung

Gibt SiteMinder die Rollen, die Aufgaben in der Finanzanwendung haben, an den Web-Agenten zurück, der dann die Informationen der Finanzanwendung übergibt.

**Hinweis:**Die *Anwendungs-ID,* die Sie liefern, sollte mit einer *Anwendungs-ID* übereinstimmen, die Sie angegeben haben, als Sie "Zugriffsaufgabe erstellen" in Identity Manager verwendet haben. Wenn Sie die Aufgabe noch nicht erstellt haben, kann die Anwendungs-ID ein von Ihnen gewählter Name sein, aber er darf keine Leerzeichen oder nicht-alphanumerische Zeichen enthalten.

Sie können mehrere Anwendungs-IDs in einer kommagetrennten Liste angeben, um das Set von Rollen und Aufgaben von mehreren Anwendungen in einem einzelnen Antwortattribut zurückzugeben. Um zum Beispiel die Liste von Rollen zurückzugeben, die ein Benutzer in Finanz- und Einkaufsanwendungen hat, geben Sie Folgendes an:

SM_USER_APPLICATION_ROLES:Finanzen, Einkauf

## Checkliste für das Aktivieren von Zugriffsrollen in SiteMinder

**Hinweis:** Die folgenden Schritte setzen voraus, dass die Anwendung, auf die sich die Zugriffsrolle, die Sie erstellen, bezieht, bereits von SiteMinder geschützt wird. Wenn Sie eine Zugriffsrolle für eine Anwendung erstellen, die nicht von SiteMinder geschützt wird, finden Sie im *Handbuch für CA eTrust SiteMinder-Richtliniendesign* Anweisungen, wie Sie die Anwendung in SiteMinder konfigurieren.

| ✓ | Schritt | Weitere Informationen finden Sie unter... |
|---|---|---|
| | 1. Weisen Sie in der Richtlinienserver-Benutzeroberfläche das Benutzerverzeichnis, das mit der Identity Manager-Umgebung verknüpft ist, einer Richtliniendomäne zu. | *CA eTrust SiteMinder-Richtliniendesign* |
| | 2. Fügen Sie die Identity Manager-Umgebung zur SiteMinder-Domäne hinzu, die die Anwendung schützt, auf die sich die Zugriffsrolle bezieht. | *CA eTrust SiteMinder-Richtliniendesign* |
| | 3. Erstellen Sie in der Richtliniendomäne Bereiche und Regeln (wenn sie bereits nicht vorhanden sind), die den Ressourcen entsprechen, auf die die Zugriffsrolle Zugriff erteilen wird. | *CA eTrust SiteMinder-Richtliniendesign* |
| | 4. Erstellen Sie eine Antwort zur Weiterleitung von Berechtigungsinformationen an die Ressource. | Erstellen einer SiteMinder-Antwort (siehe Seite 366) |
| | 5. Erstellen Sie eine Richtlinie, und ordnen Sie sie diesen Objekten zu:<br>■ Die Rolle, die Sie in Identity Manager erstellt haben.<br>■ Die Bereiche und Regeln, die Sie in Schritt 2 erstellt haben.<br>■ Die Antworten, die Sie in Schritt 4 erstellt haben. | *CA eTrust SiteMinder-Richtliniendesign* |

## Hinzufügen von Identity Manager-Umgebungen zur einer Richtliniendomäne

Um SiteMinder die Unterstützung von Zugriffsrollen zu ermöglichen, ordnen Sie eine CA IdentityMinder-Umgebung einem Benutzerverzeichnis und einer Richtliniendomäne in SiteMinder zu.

**Hinweis:** Sie müssen den der CA IdentityMinder-Umgebung zugeordneten Benutzerspeicher zur Richtliniendomäne hinzufügen, *bevor* Sie die CA IdentityMinder-Umgebung der Richtliniendomäne hinzufügen können.

**So fügen Sie eine CA IdentityMinder-Umgebung zu einer Richtliniendomäne hinzu**

1. Fügen Sie im Dialogfeld "Richtliniendomäne" in der Richtlinienserver-Benutzeroberfläche den zur CA IdentityMinder-Umgebung zugeordneten Benutzerspeicher folgendermaßen zu einer Richtliniendomäne hinzu:
   a. Wählen Sie die Registerkarte "Benutzerverzeichnisse" aus.
   b. Wählen Sie im Dropdown-Listenfeld unten auf der Registerkarte das in die Richtliniendomäne einzuschließende Benutzerverzeichnis aus.
   c. Klicken Sie auf die Schaltfläche "Hinzufügen".

      Die Richtlinienserver-Benutzeroberfläche fügt das Verzeichnis zu der in der Registerkarte "Benutzerverzeichnisse" angezeigten Liste hinzu.
   d. Klicken Sie auf "Apply" (Übernehmen).
2. Fügen Sie die CA IdentityMinder-Umgebung wie folgt zur Richtliniendomäne hinzu:
   a. Wählen Sie die Registerkarte der CA IdentityMinder-Umgebungen aus.
   b. Wählen Sie die CA IdentityMinder-Umgebung, die Sie der Richtliniendomäne zuordnen wollen, im Dropdown-Listenfeld unten auf der Registerkarte aus.
   c. Klicken Sie auf "Hinzufügen".

      Die Richtlinienserver-Benutzeroberfläche fügt Ihre Auswahl zur Liste der CA IdentityMinder-Umgebungen oben auf der Registerkarte hinzu.
3. Klicken Sie auf "OK", um die Auswahl zu speichern und das Dialogfeld zu schließen.

   Die von Ihnen ausgewählten CA IdentityMinder-Umgebungen sind nun verfügbar, wenn Sie Richtlinien erstellen.

## Erstellen einer SiteMinder-Antwort

1. Melden Sie sich bei der Richtlinienserver-Benutzeroberfläche an.
2. Führen Sie je nach Ihren Administratorrechten einen der folgenden Schritte aus:
   - Wenn Sie die Berechtigung "System- und Domänenobjekte verwalten" haben:
     a. Klicken Sie im Objektbereich auf die Registerkarte "Domänen".
     b. Wählen Sie die Richtliniendomäne aus, zu der Sie eine Antwort hinzufügen möchten.
   - Wenn Sie die Berechtigung zum Verwalten von Domänenobjekten haben, wählen Sie im Objektbereich die Richtliniendomäne aus, zu der Sie eine Antwort hinzufügen wollen.
3. Wählen Sie in der Menüleiste "Bearbeiten", "<Domänenname>", "Antwort erstellen" aus.

   Das Antwort-Dialogfeld von SiteMinder öffnet sich (siehe Antwort-Dialogfeld).
4. Geben Sie einen Namen und eine Beschreibung für die neue Antwort ein.
5. Wählen Sie im Gruppenfeld "Agententyp" das Optionsfeld "SiteMinder" aus.
6. Aktivieren Sie die Web-Agent-Option in der Dropdown-Liste im Gruppenfeld "Agententyp", und klicken Sie auf "Anwenden", um Ihre Änderungen zu speichern.
7. Klicken Sie auf "Erstellen".

   Das Editor-Dialogfeld für das SiteMinder-Antwortattribut öffnet sich.
8. Wählen Sie in der Attribut-Dropdown-Liste die WebAgent-HTTP-Header-Variable "Antwortattribut" aus.
9. Wählen Sie in der Registerkarte zur Attributeinrichtung das Optionsfeld "Benutzerattribut" aus.
10. Geben Sie im Feld "Variable" den Namen der Variable ein, die an die Anwendung übergeben wird.

    Wenn Sie zum Beispiel die Variable TASKS angeben, wird der folgende Header zur Anwendung zurückgegeben:

    HTTP_TASKS

11. Geben Sie im Feld "Attributname" das Antwortattribut folgendermaßen an:
    - SM_USER_APPLICATION_ROLES[:*Anwendungs-ID1, Anwendungs-ID2, ..., Anwendungs-IDn*] – Gibt eine Liste von Rollen zurück, die einem Benutzer zugeordnet sind
    - SM_USER_APPLICATION_TASKS[:*Anwendungs-ID1, Anwendungs-ID2, ..., Anwendungs-IDn*]

    SiteMinder-generierte Antwortattribute (siehe Seite 363) bieten weitere Informationen.
12. Klicken Sie auf "OK", um die Änderungen zu speichern und zum SiteMinder-Verwaltungsfenster zurückzukehren.

## Hinzufügen von Rollen zu einer SiteMinder-Richtlinie

Wenn ein Benutzer, dem die entsprechende Zugriffsrolle zugewiesen worden ist, versucht, auf eine geschützte Ressource zuzugreifen, überprüft der SiteMinder-Richtlinienserver, dass die Zugriffsrolle dem Benutzer zugewiesen worden ist, und löst dann die in die Richtlinie eingeschlossenen Regeln aus, um zu bestätigen, ob der Benutzer auf die Ressource zugreifen darf.

**So fügen Sie Rollen zu einer SiteMinder-Richtlinie hinzu**

1. Klicken Sie im SiteMinder-Dialogfeld "Richtlinie" auf die Registerkarte "Benutzer".

   Die Registerkarte "Benutzer" enthält Registerkarten für jede(s) in die Richtliniendomäne eingeschlossene Benutzerverzeichnis und CA IdentityMinder-Umgebung.
2. Wählen Sie die CA IdentityMinder-Umgebung aus, die die Rollen enthält, die Sie der Richtlinie hinzufügen wollen.
3. Klicken Sie auf die Schaltfläche "Hinzufügen/Entfernen".

   Das Dialogfeld für die Identity Manager-Rolle der SiteMinder-Richtlinie öffnet sich.
4. Um der Richtlinie Rollen hinzuzufügen, wählen Sie einen Eintrag aus der Liste der verfügbaren Mitglieder aus und verschieben ihn zur Liste der aktuellen Mitglieder.
5. Klicken Sie auf "OK", um die Änderungen zu speichern und zum Dialogfeld der SiteMinder-Richtlinie zurückzukehren.

## Ausschließen von Rollen in einer Richtlinie

Neben der Verwendung von Zugriffsrollen, um Zugriff auf Anwendungen zu erteilen, können Sie Zugriffsrollen auch verwenden, um zu verhindern, das Mitglieder von Zugriffsrollen auf eine Anwendung zugreifen. Um Mitglieder von Zugriffsrollen davon abzuhalten, auf eine Anwendung zuzugreifen, schließen Sie die Rollen aus den SiteMinder-Richtlinien aus. Wenn ein Benutzer, dem die ausgeschlossene Zugriffsrolle in CA IdentityMinder zugewiesen worden ist, versucht, auf eine geschützte Ressource zuzugreifen, überprüft der Richtlinienserver den Ausschluss der CA IdentityMinder-Rolle für den zugeordneten Benutzer. Nach der Überprüfung sperrt er Zugriff auf die Ressource.

**Gehen Sie wie folgt vor:**

1. Klicken Sie im SiteMinder-Dialogfeld "Richtlinie" auf die Registerkarte "Benutzer".

   Die Registerkarte "Benutzer" enthält Registerkarten für jede(s) in die Richtliniendomäne eingeschlossene Benutzerverzeichnis und CA IdentityMinder-Umgebung.

2. Klicken Sie auf die CA IdentityMinder-Umgebung, die die Rollen enthält, die Sie aus Ihrer Richtlinie ausschließen wollen.

3. Klicken Sie auf die Schaltfläche "Hinzufügen/Entfernen".

   Das Dialogfeld für die CA IdentityMinder-Rolle der SiteMinder-Richtlinie öffnet sich.

4. Um der Richtlinie Rollen hinzuzufügen, wählen Sie einen Eintrag aus der Liste der verfügbaren Mitglieder aus und klicken Sie auf den Pfeil nach links, der auf die Liste der aktuellen Mitglieder verweist.

   Der umgekehrte Vorgang entfernt Rollen aus der aktuellen Mitgliederliste.

5. Wählen Sie in der Liste der aktuellen Mitglieder die auszuschließenden Rollen aus, und zu klicken Sie auf die Schaltfläche "Ausschließen", die sich unter der Liste befindet.

   Ein roter durchgestrichener Kreis wird links von den ausgeschlossenen Rollen angezeigt.

6. Klicken Sie auf "OK", um die Änderungen zu speichern und zum Dialogfeld der SiteMinder-Richtlinie zurückzukehren.

# Konfigurieren des LogOff-URI

Um eine CA IdentityMinder-Umgebung zu schützen, konfigurieren Sie den SiteMinder-Web-Agenten, der die Umgebung schützt, sodass die Benutzersitzung beendet wird, nachdem der Benutzer sich bei CA IdentityMinder abgemeldet hat.

Der Web-Agent beendet eine Benutzersitzung, indem er die SiteMinder-Sitzungs- und Authentifizierungs-Cookies aus dem Webbrowser löscht und den Richtlinienserver beauftragt, Sitzungsinformationen zu entfernen.

Um die SiteMinder-Sitzung zu beenden, konfigurieren Sie die Abmeldefunktionalität im LogOffURI-Feld im Agent-Konfigurationsobjekt für den SiteMinder-Agenten, der die CA IdentityMinder-Umgebung schützt.

**Hinweise:**

- Ein SiteMinder-Agent hat ein LogOff-URI. Alle vom Agenten geschützten Anwendungen verwenden die gleiche Abmeldeseite.
- Wenn Sie benutzerdefinierte Abmeldeseiten in der Management-Konsole wie im Abschnitt zum Konfigurieren von benutzerdefinierten Abmeldeseiten beschrieben konfigurieren, sendet CA IdentityMinder die Abmeldeanfrage an die benutzerdefinierte Abmeldeseite *und* den LogOff-URI. Allerdings zeigt CA IdentityMinder dem Benutzer nur die benutzerdefinierte Abmeldeseite an.

**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei einer der folgenden Schnittstellen an:
   - Für CA SiteMinder r12 oder höher melden Sie sich bei der Verwaltungsoberfläche an.
   - Für CA eTrust SiteMinder 6.0 SP5 melden Sie sich bei der Richtlinienserver-Benutzeroberfläche an.

   **Hinweis:** Weitere Informationen zur Verwendung dieser Schnittstellen finden Sie in der Dokumentation der SiteMinder-Version, die Sie verwenden.
2. Ändern Sie die Eigenschaft "#LogOffUri" im Agent-Konfigurationsobjekt für den Agenten, der die CA IdentityMinder-Umgebung schützt, wie folgt:
   - Entfernen Sie das Rautenzeichen (#).
   - Geben Sie im Feld "Wert" folgenden URI an:

     /iam/im/logout.jsp

   **Hinweis:** Sie wählen ein Agent-Konfigurationsobjekt aus, wenn Sie den Web-Agenten installieren. Weitere Informationen finden Sie im *Installationshandbuch zum CA SiteMinder Web Access Manager-Richtlinienserver*.
3. Speichern Sie die Änderungen.
4. Starten Sie den Webserver neu.

## Aliasnamen in SiteMinder-Bereichen

Ein *Alias* ist eine eindeutige Zeichenfolge, die der URL hinzugefügt wird, um auf eine CA IdentityMinder-Umgebung zuzugreifen. Wenn zum Beispiel der Aliasname einer Umgebung *employees* ist, ist die URL, mit der man auf diese Umgebung zugreift, folgendermaßen:

`http://`*`myserver.mycompany.org`*`/iam/im/employees`

*myserver.mycompany.org*

Definiert den voll qualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist.

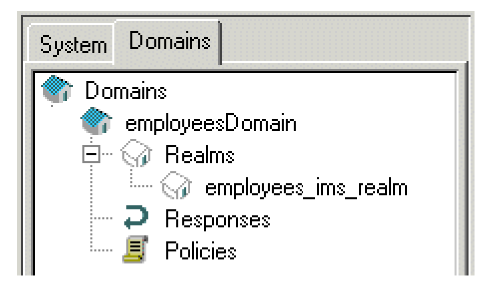
Sie geben mindestens ein Alias an, wenn Sie eine CA IdentityMinder-Umgebung in der Management-Konsole erstellen. (Sie können auch ein öffentliches Alias angeben.)

SiteMinder verwendet den Umgebungsnamen, um die Objekte zu benennen, die die Umgebung schützen. Wenn Sie den Namen *employees* angeben, erstellt SiteMinder zum Beispiel Objekte mit dem Namen *employeesobject_type*.

*object_type*

Definiert das SiteMinder-Objekt, wie employees_ims_realm.

Die folgende Abbildung zeigt zwei der Objekte, die SiteMinder erstellt:




### Aktualisieren eines Alias in SiteMinder-Bereichen

Wenn Sie das geschützte oder öffentliche Alias in der Management-Konsole ändern, versucht CA IdentityMinder, die Aliasnamen im Richtlinienserver zu aktualisieren. Wenn CA IdentityMinder die Namen nicht aktualisieren kann, können Sie sie manuell in einer der folgenden Schnittstellen aktualisieren:

- Für CA SiteMinder Web Access Manager r12 oder höher verwenden Sie die Verwaltungsoberfläche.
- Für CA eTrust SiteMinder 6.0 SP5 verwenden Sie die Richtlinienserver-Benutzeroberfläche.

**Gehen Sie wie folgt vor:**

1. Suchen Sie die Bereiche für die CA IdentityMinder-Umgebung.

   Diese Bereiche werden automatisch erstellt (mit anderen erforderlichen SiteMinder-Objekten), wenn CA IdentityMinder in SiteMinder integriert ist.

   Die Bereiche verwenden die folgende Namenskonvention:

   - *Identity Manager-Umgebung*_ims_realm – Schützt die Benutzerkonsole.
   - *Identity Manager-Umgebung*_pub_realm – Ermöglicht die Unterstützung von öffentlichen Aufgaben wie Selbstregistrierung und vergessene Kennwörter. Dieser Bereich wird nur angezeigt, wenn Sie ein öffentliches Alias konfiguriert haben.

     **Hinweis**: Wenn Sie die Richtlinienserver-Benutzeroberfläche verwenden, um den Bereich zu ändern, suchen Sie zuerst die Richtliniendomäne (*Identity Manager-Umgebung*Domain) für die CA IdentityMinder-Umgebung. Diese Bereiche befinden sich unter der Domäne.

2. Ändern Sie die Ressource für den Bereich folgendermaßen:

   /iam/im/*new_alias*

   Entfernen Sie nicht "/iam/im/", das dem Alias im Ressourcenfilter vorangeht.

3. Speichern Sie die Änderungen.

**Hinweis:** Im Abschnitt über das Ändern der CA IdentityMinder-Eigenschaften finden Sie Anweisungen, wie Sie ein Alias in der Management-Konsole ändern.

## Ändern eines SiteMinder-Kennworts oder gemeinsamen geheimen Schlüssels

Wenn Sie die CA IdentityMinder-Erweiterungen des Richtlinienservers installieren, liefern Sie das Kennwort für das SiteMinder-Administratorkonto, das CA IdentityMinder verwendet, um mit dem Richtlinienserver zu kommunizieren.

Sie können das Kennwort ändern; allerdings muss das Kennwort verschlüsselt werden. Um ein Kennwort zu verschlüsseln, verwenden Sie das Kennwort-Tool, das mit CA IdentityMinder geliefert wird.

**Hinweis:** Vergewissern Sie sich, dass die JAVA_HOME-Variable für Ihre Umgebung definiert ist, bevor Sie das SiteMinder-Kennwort ändern.

**Gehen Sie wie folgt vor:**

1. Verschlüsseln Sie das Kennwort folgendermaßen:

   a. Navigieren Sie von der Befehlszeile zu "*admin_tools*\PasswordTool", wobei *admin_tools* der installierte Speicherort der Verwaltungstools ist, wie in den folgenden Beispielen angegeben:

      - **Windows:** C:\Programme\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

      - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool

   b. Geben Sie folgenden Befehl ein:

      pwdtools *new_password*

      In diesem Befehl ist *new_password* das zu verschlüsselnde Kennwort.

      Hinweis: Geben Sie für Information zu Optionen für das Hilfsprogramm "pwdtools" den folgenden Befehl ein:

      pwdtools help

   c. Kopieren Sie das verschlüsselte Kennwort.

2. Führen Sie die entsprechenden Schritte aus:

   - Wenn CA IdentityMinder auf einem WebLogic-Anwendungsserver ausgeführt wird, gehen Sie wie folgt vor:

     a. Bearbeiten Sie in der WebLogic-Konsole den WebLogic-Ressourcenadapter im Connector-Deskriptor "policyserver_rar".

     b. Fügen Sie das verschlüsselte Kennwort als Wert der Kennworteigenschaft hinzu.

   - Wenn CA IdentityMinder auf einem JBoss-Anwendungsserver ausgeführt wird, gehen Sie wie folgt vor:

     A. Öffnen Sie "ra.xml" unter "*JBoss_home*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF".

     B. Fügen Sie das verschlüsselte Kennwort als Wert von "config-property" "Password" hinzu.

   - Wenn CA IdentityMinder auf einem WebSphere-Anwendungsserver ausgeführt wird, gehen Sie wie folgt vor:

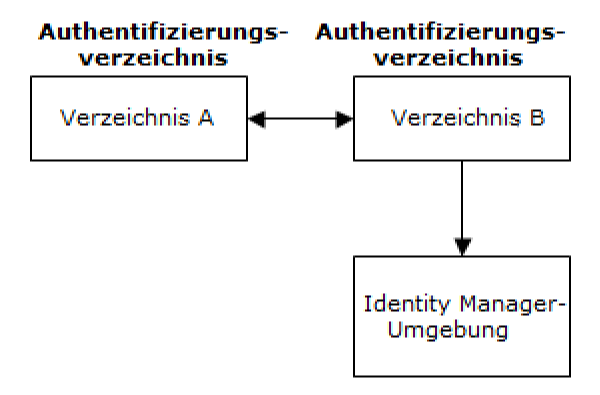
     A. Öffnen Sie in der WebSphere-Konsole "ra.xml".

     B. Fügen Sie das verschlüsselte Kennwort als Wert von "config-property" "Password" hinzu.

3. Starten Sie den Anwendungsserver neu.

## Konfigurieren einer CA IdentityMinder-Umgebung zur Verwendung von unterschiedlichen Verzeichnissen für Authentifizierung und Autorisierung

Unter Umständen muss ein Administrator Benutzer verwalten, deren Profile in einem anderen Benutzerspeicher als dem vorhanden sind, der für die Authentifizierung des Administrators verwendet wird. Mit anderen Worten, beim Anmelden ind der CA IdentityMinder-Umgebung muss der Administrator anhand eines Verzeichnisses authentifiziert werden und in einem zweiten Verzeichnis für die Benutzerverwaltung autorisiert werden, wie in der folgenden Abbildung gezeigt:




**Gehen Sie wie folgt vor:**

1. Melden Sie sich bei einer der folgenden Schnittstellen an:
   - Für CA SiteMinder Web Access Manager r12 oder höher melden Sie sich bei der Verwaltungsoberfläche an.
   - Für CA eTrust SiteMinder 6.0 SP5 melden Sie sich bei der Richtlinienserver-Benutzeroberfläche an.

   **Hinweis:** Weitere Informationen zur Verwendung dieser Schnittstellen finden Sie in der Dokumentation der SiteMinder-Version, die Sie verwenden.

2. Erstellen Sie zwei Benutzerverzeichnisse.

   Ein Verzeichnis bezieht sich auf die Authentifizierungsdaten (Administratorprofile); das andere Verzeichnis bezieht sich auf die Autorisierungsdaten (Benutzerprofile).

3. Erstellen Sie in der Management-Konsole eine CA IdentityMinder-Umgebung.

   Wählen Sie das Autorisierungsverzeichnis als das CA IdentityMinder-Verzeichnis aus.

4. Fügen Sie in der Schnittstelle für die verwendete Version von SiteMinder das Authentifizierungsverzeichnis der Domäne für die CA IdentityMinder-Umgebung hinzu, die Sie im vorherigen Schritt erstellt haben.

   Die Domäne und andere Objekte, die für SiteMinder erforderlich sind, werden automatisch erstellt, wenn Sie eine Umgebung erstellen und SiteMinder in CA IdentityMinder integriert ist.

   Die Domäne verwendet die folgende Namenskonvention:

   *Identity Manager-Umgebung*Domain

5. Vergewissern Sie sich, dass dieses Verzeichnis zuerst in der Liste von Verzeichnissen angezeigt wird, die zur Domäne zugeordnet sind.

6. Suchen Sie *Identity Manager-Umgebung*_ims_realm.

7. Ordnen Sie das Autorisierungverzeichnis zum Authentifizierungsverzeichnis im Abschnitt "Erweitert" der Bereichsdefinition zu.

8. Suchen Sie die Antwort "*Identity Manager-Umgebung*response_ims".

9. Fügen Sie den Antworten wie folgt Antwortattribute hinzu:

| **Feld** | **Wert** |
|---|---|
| Attribut | Web-Agent-HTTP-Header-Variable |
| Attributtyp | Benutzerattribut |
| Variablenname | sm_userdn |
| Attributname | SM_USERNAME |

10. Speichern Sie die Änderungen.

    CA IdentityMinder verwendet jetzt unterschiedliche Verzeichnisse für Authentifizierung und Autorisierung.

## So verbessern Sie die Leistung von LDAP-Verzeichnisvorgängen

Das Bearbeiten von Verzeichnisvorgängen kann länger dauern, weil alle CA IdentityMinder-Anfragen für das LDAP-Benutzerverzeichnis durch ein festes Set von Verbindungen geleitet werden.

Um den Durchsatz von CA IdentityMinder-Anfragen an den Benutzerspeicher zu erhöhen, konfigurieren Sie SiteMinder, um mehrere Verbindungen für das gleiche Verzeichnis zu öffnen. Fügen Sie dazu den LDAP-Server in der Richtlinienserver-Benutzeroberfläche mehrmals zum LDAP Verzeichnis-Failover und zur Lastenausgleichseinrichtung hinzu.

Wie oft Sie den LDAP-Server eingeben (und die Anzahl der zu erstellenden Verbindungen) hängt von der Last auf CA IdentityMinder ab.

# Anhang A: FIPS 140-2-Kompatibilität

Dieses Kapitel enthält folgende Themen:

<FIPS> Übersicht (siehe Seite 377)
Kommunikation (siehe Seite 378)
Installation (siehe Seite 378)
Herstellen einer Verbindung mit SiteMinder (siehe Seite 379)
Schlüsseldatei-Speicherung (siehe Seite 379)
Das Kennwort-Tool (siehe Seite 380)
FIPS-Modus-Erkennung (siehe Seite 382)
Verschlüsselte Textformate (siehe Seite 383)
Verschlüsselte Informationen (siehe Seite 383)
FIPS-Modus-Protokollierung (siehe Seite 383)

## <FIPS> Übersicht

Die FIPS-Veröffentlichung (Federal Information Processing Standards) 140-2 ist ein Sicherheitsstandard für die kryptographischen Bibliotheken und Algorithmen, die ein Produkt für die Verschlüsselung verwenden sollte. Die FIPS 140-2-Verschlüsselung wirkt sich auf die Übermittlung aller sensiblen Daten zwischen verschiedenen CA-Produktkomponenten sowie zwischen CA-Produkten und Produkten von Drittanbietern aus. In der FIPS-Veröffentlichung 140-2 sind die Anforderungen festgelegt, die erfüllt werden müssen, um innerhalb eines Sicherheitssystems zum Schutz von sensiblen, nicht klassifizierten Daten kryptographische Algorithmen zu verwenden.

CA Identity Manager verwendet den von der US-Regierung angepassten Advanced Encryption Standard (AES). CA Identity Manager integriert die kryptografischen Bibliotheken RSA Crypto-J v3.5 und Crypto-C ME v2.0, für die bestätigt wurde, dass sie die Sicherheitsanforderungen für kryptografische Module gemäß FIPS 140-2 erfüllen.

# Kommunikation

FIPS-Verschlüsselung deckt alle Datenkommunikationen zwischen CA IdentityMinder und den folgenden Komponenten ab:

- CA IdentityMinder-Server
- Bereitstellungsserver
- Bereitstellungsmanager und Clients
- C++-Connector-Server
- C++-Connector-Server-Endpunkte (falls vom Endpunkt unterstützt)
- CA IAM-Connector-Server (CA IAM CS)
- CA IAM CS-Endpunkte (falls vom Endpunkt unterstützt)
- Connector Xpress (falls vom Endpunkt unterstützt)
- Windows-Kennwortsynchronisierungs-Agenten
- Java-Identitäts- und Zugriffsmanagement (JIAM)

# Installation

Mithilfe des Identity Manager-Installationsprogramms können Sie CA IdentityMinder so konfigurieren, dass die Anforderungen gemäß FIPS 140-2 erfüllt werden.

Alle Komponenten in einer Identity Manager-Umgebung müssen für FIPS 140-2 aktiviert sein, damit Identity Manager FIPS 140-2 unterstützt. Um FIPS 140-2 während der Installation zu aktivieren, ist ein FIPS-Verschlüsselungscode erforderlich. Ein Kennwort-Tool (pwdtools.bat/pwdtools.sh) für das Generieren eines FIPS-Schlüssels befindet sich im folgenden Verzeichnis:

```
<Installationspfad>\PasswordTool\pwdtools.bat
```

**Wichtig!** Verwenden Sie in allen Installationen den gleichen FIPS 140-2-Verschlüsselungscode, und stellen sicher, dass die mit dem Kennwort-Tool generierte Schlüsseldatei gesichert ist.

# Herstellen einer Verbindung mit SiteMinder

Wenn Sie während der Identity Manager-Installation eine Verbindung mit CA SiteMinder herstellen, ist zu beachten, dass der FIPS-Modus und Produktversionskonfigurationen nur in dem in der folgenden Tabelle aufgeführten Umfang unterstützt werden:

| Identity Manager r12 | SiteMinder | SiteMinder-Version |
|---|---|---|
| Modus "Nur FIPS" | Modus "Nur FIPS" | r12 |
| Modus "Nur FIPS" | FIPS-kompatibler Modus | r12 |
| Nicht-FIPS-Modus | FIPS-kompatibler Modus | r12 |
| Nicht-FIPS-Modus | Nicht-FIPS-Modus | r6 |

# Schlüsseldatei-Speicherung

CA IdentityMinder verwendet das Dateisystem zum Speichern des FIPS-Verschlüsselungscodes. Der CA IdentityMinder-Administrator ist dafür verantwortlich, unbefugten Zugriff auf Dateien zu verhindern. Zu diesem Zweck legt er die Verzeichniszugriffsberechtigungen für bestimmte Gruppen- oder Benutzertypen fest, beispielsweise für Benutzer, die berechtigt sind, CA IdentityMinder auszuführen.

In der folgenden Tabelle ist der Speicherort der FIPS-Schlüsseldateien für jede CA IdentityMinder aufgeführt.

| Komponente | Installationsort |
|---|---|
| CA IdentityMinder-Server | *IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat<br>*IdentityMinder.ear* ist der Ort, an dem CA IdentityMinder auf dem Anwendungsserver installiert wird. |
| Bereitstellungsserver | *Bereitstellungsserverinstallation*\data\tls\keymgmt\imps_datakey |
| C++ Connector Server | *Bereitstellungsserverinstallation*\data\tls\keymgmt\imps_datakey |

# Das Kennwort-Tool

Das FIPS-kompatible Kennwort-Tool-Hilfsprogramm "pwdtools.bat" (oder "pwdtools.sh") kann während der CA IdentityMinder-Installation von der Befehlszeile den Verschlüsselungscode generieren.

Bearbeiten Sie die Datei "pwdtools.bat"/"pwdtools.sh", bevor Sie das Kennwort-Tool verwenden, und legen Sie die JAVA_HOME-Variable wie erforderlich fest.

**Wichtig!** CA IdentityMinder unterstützt keine Datenmigration oder Wiederverschlüsselung. Stellen Sie deshalb sicher, dass die Verschlüsselungscodes nach der Installation nicht geändert werden.

Dieser Befehl hat folgende Syntax:

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f <encrypting parameters file>]
```

**JSAFE**

Verschlüsselt einen einfachen Textwert unter Verwendung des PBE-Algorithmus.

**Beispiel:**

```
pwdtools -JSAFE –p mypassword
```

**Hinweis**: In früheren Versionen wurde das Kennwort für den bootstrap-Administrator als Klartext gespeichert. Wenn Sie ein Upgrade oder eine Migration auf CA IdentityMinder r12.6 SP1 oder höher durchführen, dann müssen Sie das Klartextkennwort manuell verschlüsseln. Stellen Sie sicher, dass die JSAFE-Option angegeben wird, wenn Sie das Tool verwenden, und befolgen Sie diese Schritte:

1. Nachdem Sie ein Upgrade oder eine Migration auf CA IdentityMinder r12.6 SP1 oder höher durchgeführt haben, gehen Sie zur CA IdentityMinder-Objektspeicherdatenbank, und suchen Sie folgende Tabelle: `IM_AUTH_USER`
2. Verschlüsseln Sie das Klartextkennwort, indem Sie das Kennwort-Tool mit JSAFE verwenden.
3. Ersetzen Sie den Klartext mit einem verschlüsselten Kennwort in der Tabelle.

**FIPSKEY**

Erstellt eine FIPS-Schlüsseldatei für das Installationsprogramm. Sie generieren den Schlüssel, bevor Sie CA IdentityMinder installieren.

**Beispiel:**

```
pwdtools -FIPSKEY –k C:\keypath\FIPSkey.dat
```

Dabei ist *keypath* der vollständige Pfad zu dem Speicherort, wo Sie den FIPS-Schlüssel speichern wollen.

Das Kennwort-Tool erstellt den FIPS-Schlüssel am angegebenen Speicherort. Während Installation geben Sie den Speicherort der FIPS-Schlüsseldatei für das Installationsprogramm an.

**Hinweis**: Sichern Sie den Schlüssel, indem Sie die Verzeichniszugriffsberechtigungen für bestimmte Gruppen- oder Benutzertypen festlegen, z. B. der Benutzer, der zum Ausführen von CA IdentityMinder berechtigt ist.

**FIPS**

Verschlüsseln Sie einen einfachen Textwert unter Verwendung einer FIPS-Schlüsseldatei. FIPS verwendet die vorhandene FIPS-Schlüsseldatei.

**Beispiel:**

```
pwdtools -FIPS –p firewall -k C:\keypath\FIPSkey.dat
```

Wobei *keypath* der vollständige Pfad zum FIPS-Schlüsselverzeichnis ist.

**Hinweis**: Verwenden Sie die gleiche FIPS-Schlüsseldatei, die Sie während Installation angegeben haben.

**RC2**

Verschlüsselt einen einfachen Textwert unter Verwendung des RC2-Algorithmus.

**Wichtig!** CA IdentityMinder verwendet die FIPS-Schlüsseldatei, um zu überprüfen, ob die Anwendung im FIPS-Modus oder im Nicht-FIPS-Modus starten soll. Stellen Sie daher sicher, dass die Schlüsseldatei "FIPSKey.dat" genannt wird und den folgenden Anwendungsserver-Bereitstellungspfad hat:

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

Dabei ist "iam_im.ear" im Anwendungsserver-Bereitstellungsverzeichnis, zum Beispiel:

```
jboss_home\server\default\deploy
```

# FIPS-Modus-Erkennung

Um festzustellen, ob CA IdentityMinder im FIPS-Modus oder im Nicht-FIPS-Modus ausgeführt wird, verwenden Sie die Statusseite der CA IdentityMinder-Umgebung.

Geben Sie die folgende URL in einem Browser ein, um auf die Statusseite zuzugreifen:

`http://`*`server_name`*`/idm/status.jsp`

**server_name**

Bestimmt den vollqualifizierten Domänennamen des Servers, auf dem CA IdentityMinder installiert ist, zum Beispiel myserver.mycompany.com. In diesem Beispiel lautet die vollständige URL:

http://myserver.mycompany.com/idm/status.jsp

Der FIPS-Status wird im unteren Bereich der Seite angezeigt.

**Hinweis**: Sie können auch überprüfen, ob CA IdentityMinder im FIPS-Modus ausgeführt wird, indem Sie nach der folgenden Schlüsseldatei suchen:

```
/config/com/netegrity/config/keys/FIPSkey.dat
```

Wenn diese Datei vorhanden ist, wird CA IdentityMinder im FIPS-Modus ausgeführt.

Die FIPSkey.dat-Schlüsseldatei wird vom Kennwort-Tool-Hilfsprogramm - pwdtools.bat (oder pwdtools.sh) - während der Installation von <CA idmgr> erstellt.

# Verschlüsselte Textformate

Der Algorithmusname wird dem verschlüsselten Text als ein Präfix hinzugefügt und informiert CA IdentityMinder, welcher Algorithmus für die Verschlüsselung verwendet wurde.

Im FIPS-Modus ist das Präfix {AES}. Wenn Sie beispielsweise den Text "password" verschlüsseln, ist der verschlüsselte Text ähnlich wie das folgende Beispiel:

{AES}:eolQCTq1CGPyg6qe++0asg==

Im Nicht-FIPS-Modus (oder JSAFE-Modus) ist das Präfix (Algorithmustag) je nach Algorithmus {PBES} oder {RC2}. Wenn Sie beispielsweise den Text "password" verschlüsseln, ist der verschlüsselte Text ähnlich wie folgt:

{PBES}:gSex2/BhDGzEKWvFmzca4w==

Sie können dynamische Schlüssel mithilfe der Aufgabe für geheime Schlüssel im System erstellen. Wenn Sie dynamische Schlüssel definieren, wird die Schlüssel-ID zwischen einem Algorithmustag und Tagtrennzeichen eingefügt (":"). Fehlt die Schlüssel-ID in den verschlüsselten Daten, zeigt dies an, dass hartcodierter Schlüssel für die Verschlüsselung verwendet wurde. Dies kann für Rückwärtskompatibilität verwendet werden, oder wenn keine dynamischen Schlüssel für den jeweiligen Algorithmus definiert sind.

# Verschlüsselte Informationen

Die folgenden CA IdentityMinder-Informationen werden verschlüsselt:

- Kennwörter in der Datenquellenkonfiguration für Jboss
- Informationen zum Wiederherstellen vergessener Kennwörter
- Geheimer Wert für Bereitstellungsserver-Rückruf
- Workflow-Sitzungsinformationen
- Richtlinienserver-Verbindungsinformationen

# FIPS-Modus-Protokollierung

Die folgenden CA Identity Manager-Komponenten zeigen in Protokolldateien an, ob der FIPS-Modus aktiviert ist:

- Identity Manager-Server
- Bereitstellungsserver

- C++ Connector Server
- Java Connector Server
- Bereitstellungs-Manager
- Agent für die Kennwortsynchronisierung

In allen Fällen endet der Protokolleintrag, der anzeigt, dass der FIPS-Modus aktiviert ist, mit der folgenden Zeichenfolge:

FIPS 140-2 MODE: ON

# Anhang B: Ersetzen von CA IdentityMinder Zertifikate durch SHA-2-signierte SSL-Zertifikate

SHA-2-SSL-Zertifikat-Hashing ist ein kryptografischer Algorithmus, der vom National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) entwickelt wurde. SHA-2-Zertifikate sind sicherer als alle vorherigen Algorithmen. In CA IdentityMinder können Sie SHA-2-signierte SSL-Zertifikate anstelle von Zertifikaten konfigurieren, die mit der SHA-1-Hash-Funktion signiert wurden.

**Hinweis**: Weitere Informationen zur Konfiguration von SSL-Zertifikaten finden Sie im *Installationshandbuch*.

Die folgende Tabelle zeigt den Pfad auf dem CA IdentityMinder-Server an, wo Sie die SHA-2-signierten Zertifikate speichern können:

| Zertifikate | Installationspfad | Beschreibung |
|---|---|---|
| Bereitstellungsserver-Zertifikat | [Bereitstellungsserver-Installationsverzeichnis]/data/tls/server/eta2_servercert.pem<br>[Bereitstellungsserver-Installationsverzeichnis]/data/tls/server/eta2_serverkey.pem<br>*cs_install*/ccs/data/tls/server/eta2_servercert.pem<br>*cs_install*/ccs/data/tls/server/eta2_serverkey.pem<br>*cs_install*/jcs/conf/eta2_server.p12 | Vom Bereitstellungsserver im .pem-Format und von CA IAM CS im .p12-Format verwendet (einschließlich signiertes Zertifikat, privater Schlüssel und Stamm-CA-Zertifikat).<br>**Hinweis**: Importieren Sie "eta2_server.p12" in "*cs_install*/jcs/conf/ssl.keystore" unter dem Alias "eta2_server", und entfernen Sie den vorhandenen Eintrag. Das ssl.keystore-Kennwort ist das Kennwort des Connector-Servers, das während der Installation angegeben wird. |

| Zertifikate | Installationspfad | Beschreibung |
|---|---|---|
| Bereitstellungs-Client-Zertifikat | [Bereitstellungsserver-Installationsverzeichnis]/data/tls/client/eta2_clientcert.pem<br>[Bereitstellungsserver-Installationsverzeichnis]/data/tls/client/eta2_clientkey.pem<br>[Bereitstellungsmanager-Installationsverzeichnis]/data/tls/client/eta2_clientcert.pem<br>[Bereitstellungsmanager-Installationsverzeichnis]/data/tls/client/eta2_clientkey.pem<br>*cs_install*/ccs/data/tls/client/eta2_clientcert.pem<br>*cs_install*/ccs/data/tls/client/eta2_clientkey.pem<br>*cs_install*/jcs/conf/eta2_client.p12 | Vom Bereitstellungsserver im .pem-Format und von CA IAM CS im .p12-Format verwendet (einschließlich signiertes Zertifikat, privater Schlüssel und Stamm-CA-Zertifikat). |
| Vertrauenswürdiges Zertifikat des Bereitstellungsverzeichnisses | *cadir_install*/config/ssld/impd_trusted.pem | Von CA Directory im .pem-Format verwendet. Es muss Zertifikatsinhalt in der folgenden Struktur enthalten:<br>-----BEGIN CERTIFICATE-----<br>Cert contents<br>-----END CERTIFICATE----- |
| Persönliches Zertifikat des Bereitstellungsverzeichnisses | *cadir_install*/config/ssld/personalities/impd-co.pem<br>*cadir_install*/config/ssld/personalities/impd-inc.pem<br>*cadir_install*/config/ssld/personalities/impd-main.pem<br>*cadir_install*/config/ssld/personalities/impd-notify.pem<br>*cadir_install*/config/ssld/personalities/impd-router.pem | Von CA Directory im .pem-Format verwendet. |

| Zertifikate | Installationspfad | Beschreibung |
|---|---|---|
| Root-CA-Zertifikat | [Bereitstellungsserver-Installationsverzeichnis]/data/tls/et2_cacert.pem<br>[Bereitstellungsmanager-Installationsverzeichnis]/data/tls/et2_cacert.pem<br>*cs_install*/ccs/data/tls/ et2_cacert.pem<br>*conxp_install*/lib/jiam.jar<br>[Anwendungsserver-Installationsverzeichnis]/iam_im.ear/library/jiam.jar | Zertifikat wird in Connector Xpress-Schlüsselspeicher unter "[Connector Xpress-Installationsverzeichnis]/conf/ssl.keystore" importiert.<br>Das Zertifikat muss auch in den jiam.jar-Schlüsselspeicher importiert werden. Extrahieren Sie zum Importieren die jar-Datei, importieren Sie das Zertifikat in "admincacerts.jks" und verpacken Sie dann den jar-Inhalt erneut. Das Schlüsselspeicherkennwort von "admincacerts.jks" ist "changeit". Überprüfen Sie, dass alle Kopien von "jiam.jar" ersetzt werden. |

# Nützliche Befehle

Das OpenSSL-Programm ist ein Befehlszeilentool für die Verwendung der verschiedenen Kryptografiefunktionen aus der Bibliothek von OpenSSL. Dieses Tool wird mit IMPS unter "[Bereitstellungsserver-Installationsverzeichnis]/bin" geliefert.

Die folgende Tabelle enthält einige nützliche Befehle von OpenSSL, um verschiedene Befehle für die Verwaltung von Zertifikaten auszuführen:

| Befehle | Beschreibung |
|---|---|
| `openssl x509 –in cert.pem –text –noout` | Druckt den Inhalt des .pem-Zertifikats. |
| `openssl.exe pkcs12 -in my.pkcs12 -info` | Druckt den Inhalt der .p12-Datei. |
| `openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12` | Konvertiert .pem Zert-/Schlüsselpaar zu .p12. |
| `keytool -list -v -keystore my.keystore` | Druckt den Inhalt eines Java-Schlüsselspeichers. |
| `keytool –list –v –alias myalias –keystore my.keystore` | Druckt den Inhalt eines spezifischen Alias in einem Java-Schlüsselspeicher. |

| Befehle | Beschreibung |
|---|---|
| `keytool –delete –alias myalias –keystore my.keystore` | Löscht ein Alias aus einem Java-Schlüsselspeicher. |
| `keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias` | Importiert eine .p12-Datei in einen Java-Schlüsselspeicher. |
| `keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore` | Importiert ein .pem Root-CA-Zertifikat in einen Java-Schlüsselspeicher. |